United Nations A/71/731

General Assembly

Distr.: General
13 January 2017

Original: English

Seventy-first session
Agenda item 140
Joint Inspection Unit

Fraud prevention, detection and response in United Nations system organizations

Note by the Secretary-General

The Secretary-General has the honour to transmit to the members of the General Assembly the report of the Joint Inspection Unit entitled "Fraud prevention, detection and response in United Nations system organizations".

17-00618 (E) 010217

Please recycle

JIU/REP/2016/4

FRAUD PREVENTION, DETECTION AND RESPONSE IN UNITED NATIONS SYSTEM ORGANIZATIONS

Prepared by

George A. Bartsiotas
Gopinathan Achamkulangare

Joint Inspection Unit

Geneva 2016

17-00618

Executive Summary

Fraud prevention, detection and response in United Nations system organizations
JIU/REP/2016/4

Fraud is a menace that deserves serious attention and immediate action by both the United Nations system organizations and the legislative/governing bodies. The impact of fraud in the United Nations system can be significant. In addition to substantial monetary losses, fraud has damaging effects on an organization's reputation, placing at risk the ability to implement programmes effectively, establish partnerships and receive contributions. Effective fraud prevention, detection and response mechanisms, therefore, play a key role in safeguarding organizations' interests against these negative impacts. Anti-fraud measures play an equally important role in enhancing the accountability and effectiveness of the United Nations system and in promoting appropriate oversight and the responsible use of resources.

While it is difficult to establish with reasonable certainty the global amounts lost due to fraud in the United Nations system, external and internal oversight bodies have repeatedly highlighted that the level of reported fraud is unusually low, considering the scale and complexity of the United Nations system operations and the high-risk environments in which these operations take place. Compared with fraud statistics reported by professional associations, national government entities, the private sector and academia, the level of fraud reported by the United Nations system is indeed unusually low. In broad terms, the public and private sector average is in the range of 1 to 5 per cent of total revenue, whereas it is in the range of 0.03 per cent for the United Nations system. In other words, underreporting and/or non-detection in the United nations system could be significant and endemic.

The present report addresses concerns that have been voiced by Member States and oversight bodies alike regarding the status of anti-fraud efforts in the United Nations system. It examines fraud prevention, detection and response in the United Nations system at the conceptual and operational levels, and advocates the adoption of a fraud management framework that seeks to provide guidance on ways of dealing with fraud. The report builds on the significant work done by the oversight bodies of the United Nations system in recent years, particularly by the Board of Auditors (BOA), the Independent Audit Advisory Committee (IAAC), the Office of Internal Oversight Services (OIOS) of the United Nations, and other internal and external audit bodies. JIU reports on the United Nations system also dealt in part with certain aspects of fraud, most notably the reports on the resource mobilization function (JIU/REP/2014/1), the management of implementing partners (JIU/REP/2013/4), the investigations function (JIU/REP/2011/7 and JIU/REP/2000/9), and the accountability framework (JIU/REP/2011/5).

The approach and intensity of managing the risk of fraud differ from one organization to another. Also, the nature of fraudulent activities varies widely and the levels of fraud committed by staff members and/or by external parties differ considerably among organizations. As such, the report does not advocate a "one-size-fits-all" approach to tackling fraud in the United Nations system; rather, it stresses the need to adapt the proposed fraud management framework to the requirements and

specificities of each organization. While the report does not examine in detail cases of actual fraud, it looks at the subject of fraud holistically and provides information on the approaches taken by organizations to address fraud. Special attention was paid to most fraud-prone activities and high risk environments. This includes fraud related to procurement, contract management, staff recruitment, entitlements, project management, and the selection and management of third parties such as implementing partners. Thus, the report identifies areas of common challenges and makes recommendations based on leading practices in the public and private sectors and the experiences of the multilateral organizations reviewed.

Furthermore, the report does not propose combating fraud by putting in place entirely new structures that may have serious financial implications. On the contrary, it advocates making use of the existing ones more effectively and applying proportionality to address fraud based on risk. Additionally, it emphasizes that putting in place robust fraud prevention measures would be far less costly compared to the costs of having to detect and subsequently respond to fraud that has already been perpetrated. Fraud prevention does not require armies of people to do it; rather it requires a different focus and mindset on the part of all stakeholders and particularly senior management. However, as neither can all fraud be prevented, nor can all of it be detected, a balanced approach that includes both prevention and detection is required.

In addition to addressing fraud practices across the United Nations system, the report is designed to be used as a reference for organizations to draw on information that best suits their needs and provide a roadmap for moving in the desired direction. **The report contains 16 formal recommendations, one of which is addressed to the legislative and governing bodies and 15 to the executive heads.** In addition, it contains 20 informal or "soft" recommendations, in the form of suggestions to improve policies and practices in dealing with fraud.

Much more needs to be done to combat fraud in the United Nations system

Most United Nations system entities are under pressure to address fraud not only for its direct negative impact on the internal workings of the organization, but also on account of a number of external factors: startling disclosures in the media alleging fraud; recommendations by internal and external oversight bodies; and, above all, intense pressure from the major contributors who, in turn, are subjected to similar pressure from their own supreme national audit authorities, parliaments, media, civil society and the public at large.

In such an environment, a number of United Nations system organizations have been making concerted efforts in recent years to strengthen their anti-fraud policies and strategies. Progress has been made but challenges remain; and the present review revealed that organizations need to do much better in understanding the threat of fraud and improving ways to tackle fraudulent activities and malfeasance. The challenges are manifested in several ways. The most important among them are: the absence of a strong "tone at the top" in dealing with fraud; no promotion of an encompassing anti-fraud culture; no systematic assessments to determine the level of fraud risk exposure; calling for "zero tolerance to fraud" without attempting to give it an operational content; the absence of a commonly understood definition of fraud; the absence of a clear policy and/or strategy to fight fraud; the lack of business

process ownership and serious governance deficits in dealing with fraud; delays in investigations of alleged fraud compounded by shortages of trained and qualified forensic investigators; the lack of proportionate resources dedicated to anti-fraud activities; weak implementation of multilateral frameworks for common debarment of third parties and other sanctions regimes; the lack of systematic follow-up to investigations, especially with national enforcement authorities; and the absence of a robust disciplinary regime to deal with employees engaging in fraudulent activities.

Some organizations continue to remain in a state of near denial with regard to fraud. Their inability and/or unwillingness to acknowledge and deal with the threat of fraud at the appropriate level is also reflected in comments they provided in the context of the present report. These organizations have chosen to characterize some of the main findings of the report as not relevant or applicable to their operations. Yet, while these organizations appear to be content with the systems they have in place to combat fraud, the review found these systems to be deficient in many respects. There is need for the management of these organizations to have a serious look at their fraud risk profile, acknowledge their level of exposure to fraud, and devise an effective anti-fraud programme to protect the assets, integrity, and reputation of their organizations. Most of the recommendations of the present report reflect leading practices in the anti-fraud arena and should be taken into account.

Clear understanding of fraud and presumptive fraud is essential to avoid ambiguity and support effective anti-fraud activities

There is no United Nations system-wide definition of the term "fraud". How fraud is defined and interpreted differs widely across organizations. In some cases there is lack of a common understanding of what fraud is even within the same organization. The lack of a clear definition gives rise to ambiguity and can jeopardize the effective implementation of anti-fraud activities. There is a risk that staff and managers are not aware of the kind of conduct that constitutes fraud. Especially, the entities and functions entrusted with anti-fraud mandates, such as investigators, auditors, finance departments, program managers, etc. cannot perform effectively without a clear definition of the term itself. The definition of fraud also has legal implications and affects the required level of proof and evidence for investigations, as well as the disciplinary proceedings against staff members and the sanction proceedings against third parties. Furthermore, a common definition across the United Nations system is needed to ensure compatibility and comparability of fraud data across organizations and improve transparency (see **recommendation 1**). There is also no official definition of presumptive fraud in most organizations covered by this review. The lack of clarity and a common understanding of presumptive fraud impede accurate and proper reporting in the organizations' financial statements.

~◊~

In order to provide a structured approach to realizing the objectives of the report, JIU developed a Fraud Management Framework comprising eight pillars that address prevention, detection and response to fraud in the United Nations system. Observations, findings, and recommendations in the context of these pillars are summarized below.

ANTI-FRAUD GOVERNANCE AND LEADERSHIP (PILLAR 1)

Tone at the top and a strong anti-fraud culture is fundamental to fraud mitigation

Unquestionably, the prevention and detection of and response to fraud constitute one of the primary and critical responsibilities of management and, in this sense, "the buck stops" with the executive heads. Many respondents to a JIU fraud survey conducted across the United Nations system did not perceive a clear commitment on the part of the senior management to tackle fraud in their organizations. They were also not aware of any communication or effort from management to reinforce the "tone at the top" against fraud.

It is imperative that the executive heads of organizations set a clear, unambiguous and sufficiently strong "tone" and utilize every opportunity to reiterate the organization's determination in dealing with fraud. This will have a demonstration-cum-deterrent effect. It should be made clear, internally and externally to the organization, that senior management is championing the anti-fraud policy and the related anti-fraud activities. The leadership and commitment of the executive head and the senior management is essential to combating fraud by setting the example for ethical conduct and creating an anti-fraud culture throughout the organization. Such commitment is demonstrated by putting in place a robust anti-fraud programme that includes fraud awareness initiatives and the necessary anti-fraud training, aligned with the organization's accountability and compliance framework. Commitment of proportionate resources to reflect and deal with the level of assessed fraud risk should be present to facilitate and ensure success.

Currently the responsibility for dealing with fraud-related matters is dispersed across different parts of the organization. The report calls for the designation of a senior person or team as the "business process owner" of all fraud-related activities within the organization to coordinate all such activities and oversee the ownership and responsibility structure cascading down throughout the organization (see **recommendation 3**).

Effective anti-fraud efforts are dependent on a comprehensive anti-fraud policy and governance structure that allocates clear responsibility and accountability for the prevention and detection of and response to fraud and form part of the organization's accountability framework.

Only a number of United Nations system organizations have developed specific anti-fraud policies that bring together all relevant documents and procedures to guide the anti-fraud efforts. In several organizations, anti-fraud related policies and procedures are fragmented over several rules, regulations, guidelines, policies and administrative issuances, with different policy owners and different entities responsible for their implementation. This fragmentation often creates duplication of work, loopholes and inconsistences, and jeopardizes the effective implementation of the organization's anti-fraud efforts. The review found that, even in organizations that have a corporate stand-alone anti-fraud policy, a clear definition of roles, responsibilities and accountabilities is missing and there is lack of clear guidance on how to operationalize the policy (see **recommendation 2**).

A trained anti-fraud workforce is the best ally in fighting fraud

Anti-fraud training is a major component in building an organization's fraud awareness and anti-fraud culture. While most organizations have in place mandatory ethics training, the review found that the majority of United Nations system staff has not had any specific fraud-related training in recent years. Very few organizations offer dedicated training on anti-fraud aspects, in particular for risk-prone functional areas such as procurement, and none has provided evidence of a specific anti-fraud training strategy to systematically raise awareness and address capacity and knowledge deficits on anti-fraud issues among all staff. The present report recommends that organizations enhance awareness and impart training on fraud, based on a comprehensive needs assessment and an anti-fraud training strategy. At a minimum, dedicated anti-fraud training should be incorporated into existing training plans/strategies, and staff in risk-prone functional areas should be required to take frequent refresher courses on the subject (**recommendation 4**).

FRAUD RISK ASSESSMENTS (PILLAR 2)

Understanding the nature and scale of the problem

Fraud risk assessments assist in systematically identifying where and how fraud may occur and help devising proper controls to mitigate fraud-related risks. They include identifying relevant fraud risk factors; identifying potential fraud schemes and prioritizing them based on risks; determining fraud risk appetite; mapping existing controls to potential fraud schemes and identify gaps; and testing the effectiveness of fraud prevention and detection controls. Fraud risk assessments combined with a systematic feedback and lessons learned from past or on-going fraud cases are essential in realizing an organization's exposure to fraud.

Most United Nations system organizations do not conduct systematic fraud risk assessments or consider fraud to be a corporate risk. This is indicative of a general lack of understanding of the impact of fraud on an organization's operations and the importance of fraud risk assessments in estimating the extent and level of potential fraud. A number of organizations reported that fraud risks are being assessed in the context of their overall enterprise risk management (ERM) processes. However, the review found that such processes do not always focus on fraud risk to the degree necessary, and that there is need for systematic fraud risk assessments to be an integral part of the overall ERM processes. Assessments of fraud risk form the basis for the development of proportionate anti-fraud strategies to effectively deal with fraud (see **recommendation 5**).

The present report also addresses the concepts of "risk appetite" and "zero tolerance to fraud" and the imperative of investing them with solid operational content so that they can be brought from the level of rhetoric to that of reality. The report points to the need for addressing residual fraud risks with bilateral and other donors and partners to come up with a common understanding and work out risk-sharing arrangements between organizations and contributors.

ANTI-FRAUD STRATEGIES AND ACTION PLANS (PILLAR 3)

Clear strategies and action plans are needed to operationalize the anti-fraud policy and put in place effective anti-fraud measures

The review found that, while a number of United Nations system organizations have updated or developed new policies addressing the management of fraud risk, only a few have gone further to adopt corporate anti-fraud strategies and action plans to operationalize the policies and integrate them with existing corporate risk management systems, strategic plans or operational activities. As a result, most organizations have a fragmented, often ad hoc and incoherent approach to combating fraud. Furthermore, organizations that are taking steps to address fraud in a more systematic and strategic manner have done so only recently and reported the status of their efforts as "work in progress", making it difficult for this review to assess implementation and degree of success. To assure the effective implementation of the anti-fraud policy, organizations need to develop strategies and action plans tailored to the assessed fraud risks. Organizations with significant field office operations and whose programmes are executed through third parties may put more emphasis on anti-fraud strategies on implementing partners, while others may direct their efforts primarily at internal staff. Anti-fraud strategies and action plans should address prevention detection and response measures at the strategic, operational, and tactical levels. As an organization's operating environment changes, there is need to adapt anti-fraud strategies to evolving requirements (see **recommendation 6**).

ANTI-FRAUD CONTROLS (PILLAR 4)

Anti-fraud controls should be an integral part of corporate internal control frameworks

Internal controls are a basic element of an effective accountability framework. Oversight bodies of the United Nations system have repeatedly underscored that the complex and risk-prone environment in which some organizations operate demands robust internal control frameworks with strong focus on fraud controls. The review found that only a few organizations have developed a formal and comprehensive internal control framework, and most organizations did not include formally documented processes and controls to address fraud risks. This is a key concern from the perspective of corporate fraud risk. While anti-fraud internal controls may not be enough on their own to effectively fight fraud without the presence of other supplementary anti-fraud measures, controls that target fraud form an essential part of the front lines of defence against fraudulent activities.

United Nations system organizations need to assess the effectiveness of their existing controls to counter fraud, identify any gaps, and give high priority to updating internal control frameworks as necessary to ensure that organization-wide anti-fraud controls are an integral part of these frameworks (see **recommendations 7 and 8**).

Due diligence in screening of staff and third parties is decisive in strengthening anti-fraud measures

Anti-fraud due diligence comprises activities aimed at subjecting a staff member or third party to systematic scrutiny for indications of past or present fraudulent behaviour. Due diligence measures can apply to: (a) internal staff and consultants; and (b) third parties, such as implementing partners, vendors and contractors. This due diligence is based on the understanding that it is more cost-effective to take the necessary precautions and conduct adequate screening prior to engaging a potentially fraudulent candidate as staff, or to formalizing a partnership with a third party, so as to avoid challenges afterwards, including lengthy and costly legal processes. Good practice calls for due diligence not to stop at the point of engagement, but to be extended, on a risk-basis, to continuous scrutiny and screening, at regular intervals. The report found that United Nations system organizations need to put more emphasis on anti-fraud measures such as strengthening the monitoring of high risk programmes and activities, conducting spot checks, reviews and audits, and using data-mining and data-matching techniques for preventing and detecting fraud.

Anti-fraud clauses in implementing partner agreements

Transferring the implementation of programmes and funds to implementing partners, especially in unstable and conflict environments, generates additional fraud risks. To safeguard the interests of the United Nations system, concomitant control and mitigation measures are necessary, which include robust legal instruments, i.e. implementing partner agreements and memoranda of understanding. Most United Nations system audit charters have been updated to extend the mandate of the oversight services to be able to audit or investigate third parties. However, the provisions of the agreements vary in terms of comprehensiveness, detail and robustness. Some agreements only allow for audits or inspection rights, but not investigations. Some extend the oversight rights to subcontractors of the implementing partner, but many do not. The present report reiterates the importance of revisiting standard third party legal framework agreements to ensure adequate coverage and protect the United Nations system's interests (see **recommendation 9**).

Fraud controls should be an integral part of automation systems

Information technology-based measures that automate internal controls are especially effective in improving fraud detection. Rules-based filters help to identify potentially fraudulent transactions and behaviour, data analysis supports the detection of anomalies and abnormal patterns, predictive models identify potential fraud risks, and social network analysis helps to detect cases by systematically analysing links between people and transactions. A number of United Nations system organizations have basic forms of automated controls integrated in their enterprise resource planning (ERP) systems. The present report calls upon organizations to ensure that fraud prevention and detection capabilities are an integral part of automation systems functionalities, inclusive of automated activity reporting and data-mining modules in their respective ERP systems (see **recommendation 10**).

FRAUD COMPLAINT MECHANISMS (PILLAR 5)

Comprehensive whistle-blower policies are key to an effective anti-fraud programme

The review found that whistle-blowers alone account for the uncovering of more fraud and corruption than all other measures of fraud detection combined. However, while most organizations have adopted at least basic provisions that govern whistle-blowing, instructions on hotlines and other fraud reporting mechanisms were fragmented and not easily accessible. In the majority of cases, they were neither readily available on external websites nor comprehensive and clear enough. Fragmentation can be confusing to staff when deciding which channel to use or authority to address in registering complaints and whistleblowing.

There is a need to consolidate, clarify, and make readily available basic information on whistle-blower policies to staff and third parties, including on the public websites of the United Nations system organizations. Organizations that already have a whistle-blower policy should revisit it with a view to adopting good practice benchmarks outlined in the present report. These benchmarks relate among others to the duty to report fraud and misconduct, and require fraud reporting by third parties including vendors, suppliers and implementing parties (see **recommendation 11**).

Towards a centralized intake mechanism

Most organizations have multiple channels through which a whistle-blower could report a suspected fraud case. However, there is a lack of clarity among these multiple reporting venues on how they relate to each other, which types of complaints are to be received by which office, and how cross-referencing allegations and/or informing on fraud actions should be undertaken. Furthermore, in most cases, the rules for preliminary assessment of allegations and pre-screenings are not clear or not formalized at all. The present report advocates the establishment of a central intake mechanism managed by the investigation function. At a minimum, organizations with a decentralized intake mechanism should establish an obligation for management and staff to report to a designated central authority any allegations received, ongoing cases under investigation, and action taken on closed cases. Failure to report shall be considered a violation of their staff rules and regulations (see **recommendation 12**).

Protection of whistle-blowers against retaliation builds long-term confidence among staff to report fraud

It is clear that most staff suspecting fraud would not come forward if they did not feel protected from retaliation. The review found that fear of retaliation ranks high among United Nations system staff. Retaliation can take either an active form, such as demotion and firing, or a passive form, such as the failure to renew an employment contract, exclusion from training etc. Despite the value of whistle-blowing, not all United Nations system organizations have in place comprehensive provisions for protection against retaliation. Even when policies do exist, protection provisions in many instances contain loopholes and exceptions in their coverage. Organizations should establish measures to safeguard the anonymity or confidentiality of whistle-blowers and should strengthen existing policies to make

them more effective. The present report also addresses the need for organizations to extend equal protection against retaliation to various non-staff categories, including personal services consultants, volunteers and interns.

INVESTIGATIONS (PILLAR 6)

Strengthening the investigation processes

The adequacy of resources allocated to the investigation function and the capacity of the function has been the subject of various past and ongoing reviews by internal and external oversight bodies. Stakeholders have highlighted that investigations, especially of complex cases, take too long. The management review of investigative reports and delays in determining and imposing disciplinary and other corrective action is equally a subject of concern. Because of the protracted process and the challenges that most organizations are facing in pursuing perpetrators effectively, there is a perceived sense of impunity among fraud perpetrators within the United Nations system organizations. This may result in perpetrators not being deterred from committing fraud and staff being uninclined to report fraud. The present report calls for the establishment of key performance indicators and other measures to address these issues (see **recommendation 13**).

The review also found that, in most organizations, information on fraud allegations is fragmented and systems in place do not allow for effective management of cases and proper documentation and reporting. In organizations with a substantive investigative workload, a case management system is necessary for effective planning and processing of on-going cases. Such a system would usually include information on all allegations and investigations conducted in the organization and their outcome, irrespective of whether or not they were done by the investigation office or another unit in the organization, and would provide data from the receipt of the allegation to the end of the investigation process. It would also support follow-up on the investigation reports, including disciplinary measures, sanctions and referrals of cases to national law enforcement authorities for criminal and civil procedures and asset recovery. The present report calls upon organizations to establish a case management system based on the volume, frequency and complexity of cases to support their operations.

DISCIPLINARY MEASURES AND SANCTIONS (PILLAR 7)

Challenges in pursuing perpetrators

Determination and will on the part of management are necessary to follow up on investigation reports and take action to punish fraud perpetrators, internally and externally. Without the effective enforcement of a sanctions regime, there cannot be an effective anti-fraud programme. Such a regime should include disciplinary measures for internal staff and debarment for external parties. While policies to pursue disciplinary measures appear to be in place, the review revealed that most organizations weigh the legal risks heavily when deciding if and what disciplinary measures should be imposed. The challenge mentioned most often is the "standard of proof" required by the United Nations tribunals. Following a decision by the United

Nations Appeals Tribunal that requires the establishment of "clear and convincing evidence", and thus, additional exigencies as to the quality of investigations and more robust evidence are now required.

A related issue involves the referral of cases to national enforcement authorities for prosecution. Such referrals have been mostly ineffective throughout the United Nations system. They raise many legal and political questions and need careful consideration; however, the review found that organizations do not have effective procedures in place to guide them in this respect. It is imperative to strengthen the protocols and procedures for referrals to national enforcement authorities and courts for criminal and civil proceedings, as well as for asset recovery. The present report recommends that organizations review leading practices of other multilateral institutions and decide the extent to which some aspects should be applicable to them (see **recommendation 14**).

PERFORMANCE REPORTING AND FEEDBACK (PILLAR 8)

A lacuna in information and reporting on fraud

The review found that basic information on fraud was either absent or fragmented in all the organizations reviewed. There was little, if any, information on the performance of anti-fraud activities based on specific performance indicators, the level of fraud exposure, status of compliance with anti-fraud policies, credible fraud statistics, sanctions, fraud losses and recovery of assets and lessons learned. Therefore, management and legislative bodies are deprived of having accurate and readily available information on the status of fraud in their organizations, and this hinders accountability and informed decision-making.

The present report underscores the importance of collecting, verifying and collating information relating to fraud in a thorough and systematic manner from the corporate levels, regional and country offices and other field presences. It also recommends that the task of fraud disclosure and reporting should not be left only to reports by the internal oversight bodies or be unceremoniously hidden in the pages of financial statements that are presented to external auditors. Rather, the executive heads of organizations should provide annually comprehensive management reports to their legislative and governing bodies on the overall state of affairs in regard to fraud. Consequently, the legislative and governing bodies should inscribe on their agendas a permanent or standing item relating to fraud, and review regularly the management reports presented by the executive heads on the implementation of the anti-fraud activities, as well as provide guidance and oversight on fraud related matters (see **recommendations 15 and 16**).

Anti-fraud cooperation and coordination among entities

There is need to strengthen mechanisms and procedures for enhancing cooperation and coordination among the United Nations system organizations to address fraud in a comprehensive manner and on a system-wide basis. As highlighted throughout the present report, areas for cooperation, coordination and collaboration include information-sharing on vendors and implementing partners, joint anti-fraud campaigns, sharing of training material, joint or parallel investigations, and

harmonized sanctioning of staff and third parties. While there are commendable efforts underway in certain aspects of cooperation-as indicated in the report-, there is much room for improvement for anti-fraud work among organizations. Entities such as the United Nations Development Group (UNDG), the High-level Committee on Management (HLCM), the United Nations Representatives of Investigative Services (UN-RIS) and the Representatives of Internal Audit services (UNRIAS), should provide the fora for sharing experiences on fraud-related issues, and should dedicate appropriate time in their agendas for the serious discussion the subject of fraud deserves. Fraud is present throughout the United Nations system and combating fraud is an obligation not only of individual organizations but of the United Nations system as a whole.

Recommendations

Recommendation 1

The Secretary-General of the United Nations and the executive heads of other United Nations system organizations should, in the framework of the Chief Executives Board (CEB), adopt common definitions regarding fraudulent, corrupt, collusive, coercive, and obstructive practices and present these to their respective legislative and governing bodies for endorsement. In this regard, the definitions used by the multilateral development banks should be considered for adoption. Concurrently, a joint statement with a clear and unambiguous position on fraud should be adopted by the CEB to set an appropriate "tone at the top" on a system-wide basis.

Recommendation 2

The executive heads of the United Nations system organizations, if they have not already done so, shall develop a corporate anti-fraud policy for their respective organizations or update an existing one, taking into account leading practices in the public and private sectors. The policy should be presented to the legislative and governing bodies for information, adoption and/or endorsement and should be reviewed and updated regularly.

Recommendation 3

The executive heads of the United Nations system organizations should take expeditious action to designate an overall corporate manager or entity at senior level to be the custodian of the anti-fraud policy and be responsible for the implementation, monitoring and periodic review of the policy.

Recommendation 4

On the basis of a comprehensive needs assessment, the executive heads of the United Nations system organizations should establish a dedicated anti-fraud training and fraud awareness strategy for all members of the organization. At a minimum, anti-fraud training should be mandatory for staff in functional areas most prone to fraud and staff operating in fragile and high-risk field environments.

Recommendation 5

The executive heads of the United Nations system organizations should, if they have not already done so, conduct a comprehensive corporate fraud risk assessment, as an integral part of their enterprise risk management system or as a separate exercise, addressing fraud risks at all levels of their respective organization, including headquarters and field offices, as well as internal and external fraud risks. Such assessments shall be conducted at least biennially at the corporate level, and more frequently, based on need, at the operational level.

Recommendation 6

The executive heads of the United Nations system organizations, if they have not already done so, should develop organization-specific comprehensive anti-fraud strategies and action plans for implementing their respective fraud policies. Such anti-fraud strategies should be based on the organization's corporate fraud risk assessments and shall be an integral part of the overall organizational strategies and operational objectives. Based on the level of fraud risk, proportionate resources should be dedicated to operationalize the strategies and action plans.

Recommendation 7

The executive heads of the United Nations system organizations, if they have not already done so, should initiate a review of their internal control framework to ensure that proportionate anti-fraud controls do exist and that fraud risks identified in the fraud risk assessments are adequately addressed in the internal control frameworks.

Recommendation 8

When introducing or updating statements of internal controls, the executive heads of the United Nations system organizations should ensure that the statements address the adequacy of organization-wide anti-fraud controls, in accordance with good practices and applicable international standards. In the absence of a formal statement of internal controls, executive heads should certify in their annual reports to legislative and governing bodies that their organization has in place proportionate anti-fraud controls based on fraud risk assessments, and that appropriate fraud prevention, detection, response and data collection procedures and processes exist.

Recommendation 9

The executive heads of the United Nations system organizations should instruct their legal offices to review and update the legal instruments for engaging third parties, such as vendors and implementing partners, with particular attention to anti-fraud clauses and provisions.

Recommendation 10

The executive heads of the United Nations system organizations should ensure that proportionate fraud prevention and detection capabilities are an integral

part of automation systems' functionalities, including automated activity reports and data-mining modules in their respective enterprise resource planning systems (ERPs).

Recommendation 11

The executive heads of the United Nations system organizations, if they have not already done so, should revise their whistle-blower policies with a view to adopting good practices, and extend the duty to report fraud and other misconduct to contract employees, United Nations volunteers, interns and other non-staff, as well as to third parties, including vendors, suppliers, and implementing partners.

Recommendation 12

The executive heads of the United Nations system organization, if they have not already done so, should implement the good practice of establishing a central intake mechanism for all fraud allegations in their respective organizations. In the interim, for organizations with decentralized intake mechanisms, immediate action should be taken to: (a) establish an obligation for decentralized intake units to report to a central authority any allegations received, ongoing cases under investigation and closed cases, indicating the action taken; and (b) establish formal intake procedures and guidelines, including: clear criteria for the preliminary assessment, the official, office or function authorized to make the assessment, the process to be followed and the arrangements for reporting on the results of the preliminary assessments.

Recommendation 13

The executive heads of the United Nations system organizations, in consultation with the audit advisory committees, should ensure that the investigation function of their respective organizations establishes key performance indicators for the conduct and completion of investigations, and has adequate capacity to investigate, based on a risk categorization and the type and complexity of the investigations.

Recommendation 14

The executive heads of the United Nations system organizations, in consultation with the Office of Legal Affairs (OLA) of the United Nations, and their respective legal offices, should strengthen existing protocols and procedures for referrals of fraud cases (and other misconduct) to national enforcement authorities and courts for criminal and civil proceedings, as well as for asset recovery, and ensure that referrals are done in a timely and effective manner.

Recommendation 15

The executive heads of the United Nations system organizations should present to their legislative and governing bodies on an annual basis a consolidated and comprehensive management report on the performance of anti-fraud activities, based on key performance indicators. The report shall include, inter alia, the

level of fraud exposure, status of compliance with anti-fraud policies, fraud statistics, sanctions imposed, fraud losses and recovery of assets, and lessons learned.

Recommendation 16

The legislative and governing bodies of the United Nations system organizations should: place on their respective agendas a permanent or standing item relating to fraud prevention, detection and response; review on an annual basis the consolidated and comprehensive management report presented by the executive head on anti-fraud policy and activities; and provide high-level guidance and oversight on fraud-related matters.

Contents

		Paragraphs	Page
	EXECUTIVE SUMMARY		3
	ABBREVIATIONS		19
I.	**INTRODUCTION AND BACKGROUND**	1-17	21
	A. Objectives and scope	7-11	23
	B. Methodology	12-17	24
II.	**FRAUD AND PRESUMPTIVE FRAUD**	18-34	25
	A. Defining fraud	19-27	25
	B. Defining presumptive fraud	28-34	29
III.	**A FRAUD MANAGEMENT FRAMEWORK**	35-40	31
IV.	**ANTI-FRAUD GOVERNANCE AND LEADERSHIP (PILLAR 1)**	41-78	33
	A. Fraud policy	46-56	34
	B. Assigning roles and responsibilities	57-63	36
	C. Anti-fraud culture and fraud awareness	64-78	38
V.	**FRAUD RISK ASSESSMENTS (PILLAR 2)**	79-116	43
	A. Status of fraud specific-risk assessments	83-101	44
	B. Fraud risk tolerance levels	102-110	48
	C. Fraud risk sharing	111-116	50
VI.	**ANTI-FRAUD STRATEGIES AND ACTION PLANS (PILLAR 3)**	117-123	51
VII.	**ANTI-FRAUD CONTROLS (PILLAR 4)**	124-203	53
	A. Accountability frameworks	127-130	53
	B. Internal controls	131-150	54
	C. Codes of conduct	151-157	59
	D. Financial disclosure and declaration of interest programmes	158-163	61
	E. Anti-fraud due diligence: screening of staff and third parties	164-181	63
	F. Updating legal instruments for third parties	182-188	68
	G. Automation of fraud controls	189-198	70
	H. Role of internal audit in fraud detection and control	199-203	72
VIII.	**FRAUD COMPLAINT MECHANISMS (PILLAR 5)**	204-250	73
	A. Whistle-blower policies	206-216	74
	B. Whistle-blower hotlines	217-226	77

C. Protection against retaliation 227-237 79

D. Multiplicity of reporting — centralized v. decentralized intakes 238-250 82

IX. INVESTIGATIONS (PILLAR 6) 251-290 87

A. Timeliness, capacity of and quality of investigations 254-267 87

B. Investigations of third parties and joint investigations 268-274 90

C. Proactive fraud investigations 275-285 92

D. Investigation case management system 286-290 93

X. DISCIPLINARY MEASURES AND SANCTIONS (PILLAR 7) 291-359 95

A. Disciplinary process for staff members committing fraud 292-300 95

B. Challenges of pursuing perpetrators 301-329 97

C. Vendor sanction regimes 330-338 104

D. Sanctioning of implementing partners 339-346 106

E. Sharing of information on sanctioning of third parties 347-359 108

XI. PERFORMANCE REPORTING AND FEEDBACK (PILLAR 8) 360-375 110

A. Reporting on anti-fraud data and activities 360-369 110

B. Lessons learned and feedback 367-369 112

C. Audit and investigation functions interface 370-374 113

D. Anti-fraud cooperation and coordination among entities 375 114

ATTACHMENTS

1. Fraud losses and numbers as reported in the financial statements to the organizations' external auditors from 2008 to 2014 116

2. Overview of actions to be taken by participating organizations on the recommendations of the Joint Inspection Unit 120

ANNEXES

Annexes I-IV are published only on the JIU website (www.unjiu.org) together with the report

I. Compilation of fraud policies and other anti-fraud related policies

II. Definitions of fraud and presumptive fraud

III. Fraud risk assessments

IV. Survey methodology

ABBREVIATIONS

ACFE	Association of Certified Fraud Examiners
BOA	United Nations Board of Auditors
CEB	United Nations System Chief Executives Board for Coordination
COSO	Committee of the Sponsoring Organizations of the Treadway Commission
ERM	Enterprise risk management
ERP	Enterprise resource planning
FAO	Food and Agriculture Organization of the United Nations
HLCM	High-level Committee on Management
IAAC	Independent Audit Advisory Committee
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
ICSC	International Civil Service Commission
IIA	Institute of Internal Auditors
ILO	International Labour Organization
IMO	International Maritime Organization
IPs	Implementing Partners
ITU	International Telecommunication Union
JIU	Joint Inspection Unit
MDBs	Multilateral development banks
MPF	Model Policy Framework
NGO	Non-governmental organization
OIG	Office of the Inspector General
OIOS	Office of Internal Oversight Services
OLA	Office of Legal Affairs
OLAF	European Anti-Fraud Office
UNFPA	United Nations Population Fund
UNGM	United Nations Global Marketplace
UNICEF	United Nations Children's Fund

UNIDO	United Nations Industrial Development Organization
UNOPS	United Nations Office for Project Services
UN-RIS	United Nations Representatives of Investigative Services
UNRWA	United Nations Relief and Works Agency for Palestine Refugees in the Near East
WFP	World Food Programme
WHO	World Health Organization
WIPO	World Intellectual Property Organization
WMO	World Meteorological Organization
UNDG	United Nations Development Group
UNDP	United Nations Development Programme
UNEP	United Nations Environment Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNHCR	Office of the United Nations High Commissioner for Refugees
UNODC	United Nations Office on Drugs and Crime
UNOPS	United Nations Office for Project Services
UNWTO	World Tourism Organization
UPU	Universal Postal Union

I. INTRODUCTION AND BACKGROUND

1. Although the phenomenon of fraud has been known to the United Nations system organizations for decades, it has acquired a salience in recent years owing to many factors, including Members States' interest in how the United Nations system entities approach the management of fraud risk, the pressures of having to operate in fragile environments and conflict and post-conflict situations, huge expansion in humanitarian and disaster relief operations, the consequent awareness of enhanced fraud-related risks, and heightened public interest.

2. The impact of fraud occurring in any United Nations system organization can be significant. In addition to potential monetary losses, fraud has damaging effects on an organization's reputation, placing at risk the ability to implement programmes effectively, establish partnerships and receive contributions. Fraud prevention, detection and response mechanisms, therefore, play a key role in safeguarding organizations' interests against these negative impacts. Anti-fraud measures play an equally important role in enhancing the accountability and effectiveness of the United Nations system and in promoting appropriate oversight and the responsible use of resources.

3. In a recent report, the United Nations Board of Auditors (BOA) highlighted that the level of reported fraud in the United Nations is unusually low considering the scale and complexity of global United Nations activity and the high-risk environments in which that activity takes place.[1] Internal and external audit bodies throughout the United Nations system, reported that organizations lack rigorous mechanisms to assess the potential exposure to fraud and are deficient in strategies and action plans to counter fraud. Concerns have also been raised as to the investigative capacity of organizations to address fraud committed by external parties, such as implementing partners, and the lack of a coordinated approach to combat fraud related to programmes extending across organizational boundaries.

4. It is well acknowledged that estimating fraud losses in an organization is inherently difficult because of the lack of information and appropriate measuring instruments. For example, relying on fraud detection rates assumes full detection, and relying on opinion surveys is dependent on the accuracy of people's perception.[2] However, compared with worldwide fraud statistics reported by the Association of Certified Fraud Examiners (ACFE),[3] the Centre for Counter Fraud Studies of the University of Portsmouth[4] and a number of national government entities, the level of fraud reported by the United Nations system is indeed unusually low. In broad terms, the global average in the public and private sectors is in the range of 1-5 per cent of total revenue, whereas it has been in the range of 0.03 per cent of expenditure in the United Nations over the period of the past

[1] Financial report and audited financial statements for the biennium ended 31 December 2013 and report of the Board of Auditors, vol. I (A/69/5 (Vol. I)).

[2] See Jim Gee, Mark Button and Graham Brooks, *The Financial Cost of Healthcare Fraud: What the Latest Data from around the World Shows* (2011), pp. 3 ff.

[3] See ACFE, *Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study* (Austin, Texas, 2016).

[4] "Measuring fraud in overseas aid", March 2012, Center for Counter Fraud Studies, University of Portsmouth.

10 years.[5] In other United Nations system organizations, it is similarly low as indicated in table 1 below. It should be noted that a number of organizations report zero fraud losses in their annual financial statements to external auditors. Attachment 1 to this present report provides additional details of the fraud-related losses reported by United Nations system organizations in the financial statements to their external auditors.

Table 1: Examples of total fraud losses and percentages for years 2008-2014

Organization	Total amount of fraud, US$	Fraud losses against total expenditure, per cent
UN Secretariat	13,272,434	0.0325
UNDP	19,125,269	0.0595
UNEP	953,842	0.0696
UNFPA	434,055	0.01
UN-Habitat	356,444	0.0258
UNHCR	678,485	0.0041
UNICEF	7,805,958	0.025
UNODC	56,022	0.0032
UNOPS	521,950	0.0175
UNRWA	209,879	0.0033
UN-Women	667,548	0.0632
WFP	3,735,451	0.0122
UNIDO	€ 19,123	0.0054

Source: As reported in the financial statements to the organizations' external auditors.

5. In addressing fraud-related concerns, United Nations system organizations have been making efforts in recent years to update and enhance their anti-fraud policies, procedures and strategies. Despite the progress made, challenges remain and stakeholders acknowledge[6] that the United Nations system needs to do better in understanding the threat of fraud and improving ways to tackle fraudulent activities and malfeasance. The results of the Joint Inspection Unit (JIU) interviews, the analysis of data, and the fraud surveys conducted for the present report suggest that fraud is a menace that deserves serious attention and immediate action by both the United Nations system organizations and the legislative/governing bodies.

6. JIU has done work in previous years on management topics that addressed fraud-related issues, such as JIU reports on oversight and accountability,[7] the

[5] Concise summary of the principal findings and conclusions contained in the reports of the Board of Auditors for the biennium 2012-2013 and annual financial periods 2012 and 2013 (A/69/178), para. 62.

[6] The fraud topic was ranked highly by JIU participating organizations during prioritization of the JIU programme of work for 2015.

[7] Oversight lacunae in the United Nations system (JIU/REP/2006/2); The audit function in the United Nations system (JIU/REP/2010/5); Accountability frameworks in the United Nations system (JIU/REP/2011/5).

investigations function,[8] issues of corporate ethics[9] and the management of implementing partners.[10] However, JIU had not undertaken to date a fully-fledged review specific to the issue of fraud prevention, detection and response.

A. Objectives and scope

7. The main objective of this review was to assess the fraud risk management programmes of United Nations system organizations and the implementation of anti-fraud policies and procedures in allowing effective prevention, detection and response to fraud. The review focused on identifying areas of strengths and weaknesses and making recommendations with a view to improving overall effectiveness of the United Nations system organizations in combating fraud.

8. The review was undertaken on a United Nations system-wide basis inclusive of the United Nations, the funds and programmes, specialized agencies and the International Atomic Energy Agency at a global, interregional and national level. Specifically, the review examined the organizations' anti-fraud governance frameworks; fraud risk assessments; prevention and detection controls and response mechanisms; fraud awareness programmes; internal and external monitoring and reporting systems; investigative methods; and the disciplinary systems in place for dealing with fraud. In addition, the review examined the extent to which the anti-fraud policies of the United Nations system organizations are coherent and comparable, considered system-wide efforts on coordination and cooperation related to fraud prevention and detection and sought to identify good practices across the United Nations system.

9. In the present report, JIU does not examine in detail cases of actual fraud or the numerous types of fraudulent activities, but looks at the subject of fraud holistically. However, special attention was paid during the review on fraud issues related to fraud-prone activities and high risk environments. This includes fraud related to procurement, contract management, human resources management, programme and project management, financial management, entitlements and the selection and management of third parties, such as implementing partners.

10. The review took into account that United Nations system organizations have diverse and globally dispersed operations, and that their management systems have been designed to accommodate their mandates, business models and the environment in which they operate. Consequently, organizations have chosen tailored approaches to addressing and mitigating fraud risks and related activities. Consideration was given to the fact that fraudulent activities vary widely and the levels of fraud committed by staff members and/or by entities external to the organizations vary considerably from one organization to another. In the present report, JIU attempts to give information on the various approaches taken by organizations to fight fraud. Thereby, it identifies areas of common challenges and

[8] Strengthening the investigations function in United Nations system organizations (JIU/REP/2000/9); The investigations function in the United Nations system (JIU/REP/2011/7).
[9] Ethics in the United Nations system (JIU/REP/2010/3).
[10] Review of the management of implementing partners in United Nations system organizations (JIU/REP/2013/4).

makes recommendations as appropriate. Such recommendations may not apply equally to all organizations that participated in the review.

11. In order to provide a structured approach in achieving the objectives of the review, JIU developed a Fraud Management Framework as a road map to addresses prevention, detection, and response to fraud in the United Nations system (see chapter III below).

B. Methodology

12. The review was undertaken from March 2015 to December 2015 on a system-wide basis, including the United Nations, its funds and programmes and specialized agencies.

13. A methodology comprising desk reviews, detailed questionnaires, system-wide interviews and an anonymous global survey of staff at all levels was used to facilitate information-gathering and analysis of the subject matter. The project began with a review of the available literature on fraud, United Nations-specific documents and fraud reports and an analysis of the issues identified therein. The data collection included information received in meetings conducted at headquarter offices of participating organizations and in field visits to selected country offices in Haiti, Kenya, Panama and Thailand. Teleconferences were conducted when on-site visits were not possible. In total, more than 380 persons were interviewed. Detailed questionnaires were sent to 28 participating organizations and responses were received from 27 of them. In addition, an anonymous fraud perception survey was conducted throughout the United Nations system addressed to staff at large, with 15,929 staff responding to the survey (confidence level of 99.26 per cent). A fraud survey was also addressed to executive managers and their immediate senior staff, with 164 managers responding (confidence level of 94.10 per cent). The results of the surveys are highlighted throughout the present report. Annex IV provides the fraud survey methodology.

14. The data collection phase also included information received from the World Bank, the Inter-American Development Bank, the International Fund for Agricultural Development, the European Commission, the European Anti-Fraud Office (OLAF), the National Audit Office of the United Kingdom of Great Britain and Northern Ireland, the Government Accountability Office of the United States of America and the Global Fund. A number of development agencies of Member States were also contacted (e.g. the United Kingdom Department for International Development and the United States Agency for International Development); however, gathering the perspectives and views of a wider range of donor agencies was not feasible.

15. Time constraints and limited resources did not allow for more in-depth testing and face-to-face interactions with all 28 organizations. As such, the review took into account evidence reported in fraud-related audits conducted by the Office of Internal Oversight Services (OIOS), the BOA, the Independent Audit Advisory Committee (IAAC), and a number of other internal and external oversight bodies of United Nations system organizations. Given the wide scope and diverse nature of the topic, the Inspectors found the information from these reports invaluable and appreciate the cooperation and information provided by the United Nations system

internal and external audit community for the review. Special thanks are due to the directors of audit and oversight offices at the United Nations/OIOS, the Food and Agriculture Organization of the United Nations (FAO), UNFPA, the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), the World Intellectual Property Organization (WIPO), UNOPS, the World Health Organization (WHO), UNICEF, and the Pan American Health Organization (PAHO), as well as the Division for Treaty Affairs of UNODC, who showed keen interest in this important subject and provided valuable input on conceptual matters during the course of the review.

16. An internal peer review procedure was used to solicit comments from all JIU Inspectors (Collective Wisdom) before the report was finalized. The draft report was also circulated to United Nations organizations and other stakeholders for correction of factual errors and for comments on the findings, conclusions and recommendations. To facilitate the handling of the report, the implementation of its recommendations and monitoring thereof, Attachment 2 to the present report contains a table indicating whether the report is submitted for action or for information to the governing bodies and executive heads of the organizations reviewed.

17. The Inspectors wish to express their appreciation to all who assisted them in the preparation of the present report and in particular to those who participated in the interviews, questionnaires and surveys, and so willingly shared their knowledge and expertise.

II. FRAUD AND PRESUMPTIVE FRAUD

18. Following best practices, organizations should have in place a clear understanding of the terms "fraud" and "presumptive fraud" to avoid ambiguity and support effective implementation of anti-fraud activities. In the first place, managers and staff need to be made aware of what constitutes fraud and presumptive fraud, and the types of misconduct that are prohibited in their work environment. Equally, the entities and functions entrusted with anti-fraud mandates, such as investigators, auditors, finance departments, programme managers and human resources departments, need to have a clear understanding of the terms to effectively discharge their anti-fraud responsibilities. A clear definition also has significance for reporting on fraud and presumptive fraud by the organizations' external auditors. The definition of the terms has legal implications and impacts the required level of proof and evidence for investigations, as well as subsequent disciplinary proceedings against staff members or sanction proceedings against third parties, such as vendors, suppliers and implementing partners.

A. Defining fraud

19. Fraud definitions vary throughout the private and public sectors, as well as in academia. Black's Law Dictionary defines fraud as "a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her

detriment".[11] Similarly, ACFE[12] defines fraud as "any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain".[13] The definition given by the International Standards on Auditing (ISA) is that of "an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage".[14] The Panel of External Auditors of the United Nations, the Specialized Agencies and the International Atomic Energy Agency, addressed the term "fraud" in an audit guide issued in 1996, as "an intentional act by one or more individuals among management, employees, or third parties, which results in a misrepresentation of financial statements. While other bodies define fraud in similar terms to the above, it is generally acknowledged that underlying the definition of fraud is the notion of intention and deception as the principle modus operandi when a fraudulent act is committed. Fraud covers a wide range of behaviour that includes, inter alia, manipulation, falsification or alteration of records or documents; misappropriation of assets; suppression or omission of the effects of transactions from records or documents; recording of transactions without substance; and misapplication of accounting policies."[15]

20. It should be noted that the terms 'fraud' and 'corruption' are often lumped together and sometimes used interchangeably in the reports and documents of the United Nations system as well as in the literature of other public and private domains. Although there are instances where a particular conduct may constitute both fraud and corruption — and certainly either fraud or corruption is often described as "fraudulent acts" — it should be noted that as a legal matter the concepts remain distinct. Corruption is traditionally understood to comprise any act or omission that misuses official authority, or seeks to influence the misuse of official authority, in order to obtain an undue benefit. However, while corruption by an official could result in financial losses to the organization and would be classified as fraud, corruption may not necessarily have an impact on the organization or a person suffering a monetary loss. For example, a government official that spends donor's money by directing the benefits only to its own political constituency (instead of the population at large as intended) would not necessarily be committing fraud but the act would be considered corruption. On the other hand if the official uses some of the funds to renovate his private residence, that is an example of both corruption and fraud. **The present report focuses on the subject of fraud in the United Nations system while taking into account that fraud and**

[11] Bryan Garner, ed., *Black's Law Dictionary*, 8th ed. (2004), s.v., "fraud."

[12] See ACFE website, www.acfe.com/fraud-101.aspx (accessed 15 December 2015).

[13] Definition as presented in IIA, American Institute of Certified Public Accountants and ACFE, *Managing the Business Risk of Fraud: A Practical Guide* (2008), p. 5; it notes that that definition of fraud was developed uniquely for that guide, and the authors recognize that many other definitions of fraud exist, including those developed by the sponsoring organizations and endorsers of that guide.

[14] International Standard on Auditing 240 (redrafted), para. 11.

[15] Panel of External Auditors of the United Nations, the Specialized Agencies and the International Atomic Energy Agency, Audit Guide No. 204, issued in December 1996, pp. 1-2; this definition was also used as the Panel decided to take account of the standards issued by the International Auditing Practices Committee and Public Sector Committee of the International Federation of Accountants.

corruption are two overlapping prohibitive acts. As such, references made to fraud throughout this report may also cover aspects of corruption as applicable.

21. There is no United Nations system-wide definition of fraud and, as seen in annex II to the present report, United Nations system organizations define fraud in different ways. Furthermore, the interpretation of the term varies widely and in some organizations there is no published official definition of the term. The interviews revealed that, in some cases, there is a lack of a common understanding of the term even within the same organization. It is also notable that, when definitions do exist, they tend to borrow from the basic tenets found in the aforementioned definitions by the ACFE, the ISA, and the Panel of External Auditors, but also in the norms and standards of other international professional audit and investigation bodies, such as the Institute of Internal Auditors (IIA) and the International Federation of Accountants and the Chartered Institute of Public Finance and Accountancy. In some organizations, the definition of fraud is broad so as to capture all types of unethical behaviour and conduct, in others the definition is narrower and addresses only misrepresentation of financial statements and misrepresentations in other documents and statements. Organizations such as UNHCR, WFP, and WHO, publicize a list of examples on the types of misconduct that they consider as fraudulent.

22. The Office of Legal Affairs (OLA) of the United Nations secretariat, in an inter-office memorandum of May 2015, states that fraud is a type of criminal conduct that may be defined differently by various Member States and that it can only be proven with legal certainty by competent national authorities. In the context of the type of frauds that should be reported to the external auditors, OLA refers to General Assembly resolution 62/63 and states that "the organization report to the BOA, under the category of fraud, allegations that have been the subject of internal investigation, conducted by OIOS or other units and offices, and found to be credible". While this information clarifies which frauds should be reported to external auditors, it does not provide for a definition of fraud. **The Inspectors acknowledge that legally whether an act is in fact fraud is a determination to be made through the judicial or other adjudicative systems. However, they are of the view that a definition of fraud is essential for a common understanding of the concept within an organization. Furthermore, a common definition among United Nations system organizations, promulgated by a competent authority, would be a great advantage, as it would facilitate comparability of fraud data, patterns and trends across the United Nations system.**

23. Similarly, the Advisory Committee on Administrative and Budgetary Questions (ACABQ) in its October 2015 report highlighted the need for a single agreed definition of what constitutes fraud in order to develop effective counter-fraud policies and to ensure compatibility and comparability of related data across the United Nations system to improve the level of disclosure and transparency of cases vis-à-vis Member States, donors and staff.[16]

24. A number of United Nations system organizations, such as FAO, WIPO, WFP, UNFPA, and UNICEF, have adopted the definition of fraudulent practices used by

[16] A/70/380 of 9 October 2015, para. 30.

the multilateral development banks (MDBs) (see box 1 below). Furthermore, the United Nations Development Group (UNDG) has also endorsed the MDBs definitions of fraud and related practices as part of the standard legal agreements that govern so-called pass-through funds.[17]

25. The MDBs common definition of prohibitive practices (fraudulent, corrupt, coercive, collusive, and obstructive), are contained in the Uniform Framework for Preventing and Combating Fraud and Corruption (box 1).

Box 1: Definitions of prohibitive practices adopted by MDBs

MDBs have agreed in principle on the following standardized definitions of prohibitive practices for investigating such practices in activities financed by their institutions:

• A fraudulent practice is any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation.

• A corrupt practice is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party.

• A coercive practice is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party.

• A collusive practice is an arrangement between two or more parties designed to achieve an improper purpose, including influencing improperly the actions of another party.

• An obstructive practice[18] is (a) deliberately destroying, falsifying, altering or concealing evidence material to the investigation or making false statements to investigators in order to materially impede an investigation into allegations of a corrupt, fraudulent, coercive or collusive practice; and/or threatening, harassing or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation; or (b) intentionally acting to materially impede the exercise of the Bank's contractual rights of audit and investigation or access to information.

Each of the member institutions will determine implementation within its relevant policies and procedures, and consistent with international conventions.[19]

[17] UNDG, standard memorandum of understanding for using pass-through fund management, 26 June 2015, sect. VII. Pass-through funds include the "Delivering as One" funds, UNDG multi-donor trust funds and joint programmes, which channel about US$ 1 billion per year.

[18] The definition of "obstructive practices" was introduced at a later stage by some MDBs to supplement the original 2006 definitions of fraudulent, corrupt, coercive, and collusive practices.

[19] African Development Bank, Asian Development Bank, European Bank for Reconstruction and Development, European Investment Bank, International Monetary Fund, Inter-American Development Bank and World Bank, *Uniform Framework for Preventing and Combating Fraud and Corruption* (2006).

26. The approach adopted by MDBs has a number of advantages, as it facilitates joint efforts in preventing, detecting and responding to fraud, including better sharing of information, cooperation and coordination in conducting investigations, as well as in sanctioning fraudulent individuals and entities, i.e. third parties such as vendors, non-governmental organizations (NGOs) and other implementing partners. It is also a prerequisite for cross-debarment of vendors, suppliers and other third parties (see chapter X below). The MDBs' definitions have been in place since 2006 and reportedly they have been well established among the international financial community, as well as external parties dealing with the MDBs.

27. The implementation of the following recommendation is expected to assure a common understanding of the term fraud within the respective organization, facilitate comparability of fraud data, patterns and trends across the United Nations system and improve reporting on fraud.

Recommendation 1

The Secretary-General of the United Nations and the executive heads of other United Nations system organizations should, in the framework of the Chief Executives Board (CEB), adopt common definitions regarding fraudulent, corrupt, collusive, coercive, and obstructive practices and present these to the respective legislative and governing bodies for endorsement. In this regard, the definitions used by the multilateral development banks should be considered for adoption. Concurrently, a joint statement with a clear and unambiguous position on fraud should be adopted by the CEB to set an appropriate "tone at the top" on a system-wide basis.

B. Defining presumptive fraud

28. The term "presumptive fraud" has not been officially defined by any United Nations organization that participated in this review. The Inspectors were informed that a definition of this term does not appear in any United Nations documents and the term itself appears only in the annex to the Financial Regulations and Rules of the United Nations, entitled, "Additional terms of reference governing the audit of the United Nations". However, the Panel of External Auditors of the United Nations, the Specialized Agencies and the International Atomic Energy Agency in 1996 noted that "the term 'presumptive fraud' refers to a fraud which, though not established clearly on documentary or testimonial evidence as having been committed by the perpetrator, causes loss of valuable resources to the organization".[20] However, JIU could not determine if this definition is still in use by the Panel.

29. Some organizations chose to provide their own interpretation of presumptive fraud. For example, UNFPA defines it as "allegations which are credible and specific enough and warrant a full-fledged investigation which has not yet been concluded". For the purpose of reporting to BOA, the United Nations Development Programme (UNDP) interprets presumptive fraud as "any allegation or current

[20] Panel of External Auditors of the United Nations, the Specialized Agencies and the International Atomic Energy Agency, Audit Guide No. 204, issued in December 1996, p. 2.

investigation of fraud which appears to have resulted in a financial loss to the organization and has not yet been substantiated or closed due to lack of evidence of wrongdoing".[21] The definition of "presumptive fraud" set forth by WFP is based on that of the Panel of External Auditors as described above. The Internal Oversight Services at the United Nations Industrial Development Organization (UNIDO) interprets "presumptive" as fraud allegations "likely to be true, based on the facts established by an investigation, but not yet confirmed by the judgement/decision of the Director General". At IAEA, "presumptive" frauds are considered "alleged" frauds and are investigated based on a preliminary assessment of the existence of enough specific evidence and the type and gravity of the event reported.[22]

30. OLA in May 2015 undertook to address presumptive fraud as follows: "With respect to 'presumptive fraud', we are unaware of any guidance provided by the General Assembly in any similar circumstance that may aid OLA's interpretation. Accordingly, our only observation would be that this term appears to connote a lower threshold than fraud, and could be interpreted to encompass anything from inexplicable financial irregularities to non-frivolous suspicions of fraud that merit further investigations." Most interviewees contacted for the present report were uncertain how to interpret the aforementioned definition.

31. Lack of clarity of the term "presumptive fraud" and lack of a common understanding among organizations impedes the proper reporting on fraud cases to the external auditors.[23] **Presumptive fraud-related information is not being measured and/or collected consistently in the various United Nations system organizations and information provided to external auditors may lack accuracy and thoroughness.** Similar observations were made in the most recent BOA report, as well as a 2014 OIOS report on fraud reporting in the United Nations Secretariat.[24]

32. The Inspectors hold the view that for the purpose of reporting "presumptive fraud" in the financial statements of organizations, the term "presumptive fraud' should not necessarily be approached from a legal perspective, but rather as a financial term, which should be interpreted in line with public accounting standards and may include cases of suspected or possible fraud that, if subsequently proven, may have an impact on the organization's financial statements.

---

[21] UNDP response to JIU questionnaire.

[22] As defined in responses to JIU questionnaire.

[23] Most external auditors of United Nations system organizations are mandated to report to their legislative bodies cases of fraud and presumptive fraud as part of their annual financial report and audited financial statements. However, the primary responsibility for preventing and detecting fraud rests with management. As such, external auditors make enquiries of management for assessing the risks of material fraud and the processes in place for identifying and responding to the risks of fraud, and query whether management has any knowledge of any actual, suspected or alleged fraud. Management usually has procedures in place to collect such information, with controllers being the focal points, in most cases, for compiling fraud-related data based on the information received from investigation offices and/or collected directly from the various entities within the organization.

[24] See e.g. OIOS, audit of the process of reporting cases of fraud or presumptive fraud in financial statements, report 2014/051; concise summary of the principal findings and conclusions contained in the reports of the Board of Auditors for the annual financial period 2014 (A/70/322), paras. 52-53.

33. Many interviewees were receptive to the introduction of a common definition of fraud and presumptive fraud among United Nations system organizations. It was mentioned that attempts to this effect were made in 2005 at the CEB/High-level Committee on Management (HLCM) level by a working group established to address fraud,[25] but the work of the group was discontinued. No documentation was provided to the Inspectors for a review of the work conducted by this group and no explanation was offered or reasons adduced by HLCM as to why this effort was terminated.

34. **It is recommended that the Secretary-General of the United Nations and the executive heads of other United Nations system organizations should, in the framework of the CEB, adopt a common definition of presumptive fraud for the United Nations system. The following interpretation of presumptive fraud for the purpose of reporting in the financial statements should be considered: "Credible fraud allegations that warrant a fully-fledged investigation which has not yet been concluded and, if proven, would establish loss of valuable resources to the organization and may lead to misrepresentation of the financial statements."**

III. A FRAUD MANAGEMENT FRAMEWORK

35. As discussed in chapter I, in order to provide a structured way in reaching the objectives of this review, JIU introduced a Fraud Management Framework, necessary for an effective approach to fraud prevention, detection and response in the United Nations system. In the development of the Framework, JIU benefited from publications on work done on fraud risk and control frameworks, as well as guides and anti-fraud practices by a number of bodies in academia and the public and private sectors.[26] While these publications and practices provide guidance for effective approaches to combating fraud, they may not necessarily address issues specific to the audience of the present report. The Framework was thus developed to provide a roadmap for addressing anti-fraud activities in United Nations system organizations and potentially provide an assessment tool for future benchmarking.

36. United Nations system organizations have different mandates and business models and operate in environments that pose different fraud risks. As such, not all organizations adopt the same approach in combating fraud. Organizations may choose to take into account the principles and practices addressed in the Framework throughout the present report, as a basis for updating or developing their own robust anti-fraud strategies and management approaches based on their specific needs and requirements.

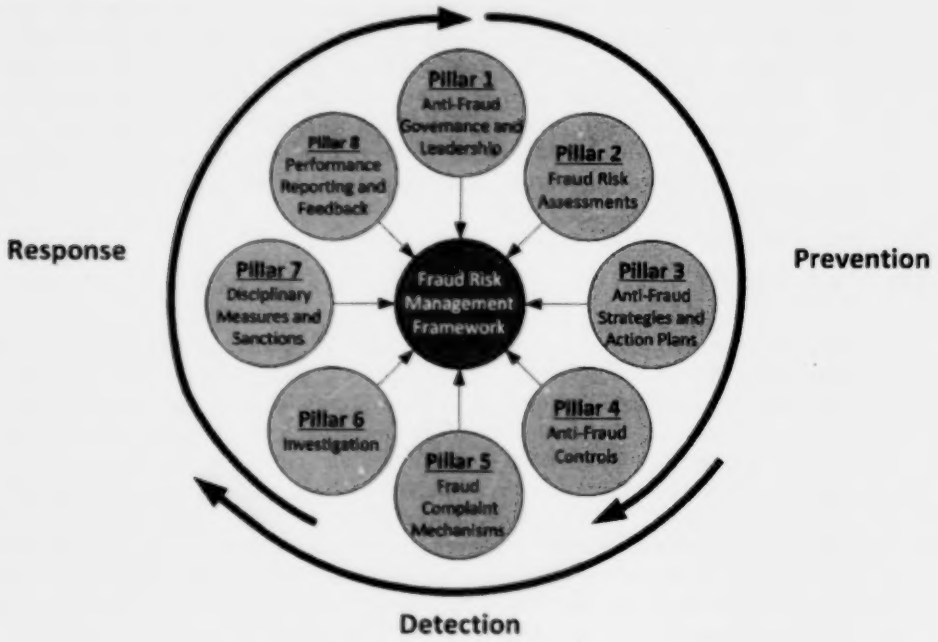
37. As depicted in the arrows of figure 1 below, the Framework addresses three categories of anti-fraud activities — prevention, detection and response — that

[25] See CEB Finance and Budget Network, Report of the Working Group on Fraud, document CEB/2005/HLCM/20.

[26] IIA, American Institute of Certified Public Accountants and ACFE, *Managing the Business Risk of Fraud: A Practical Guide* (2008); United States, Government Accountability Office, *A Framework for Managing Fraud Risks in Federal Programs* (2015); the Australian National Audit Office, *Fraud Control in Australian Government Entities: Better Practice Guide* (2011); and others.

should be encompassing any credible anti-fraud programme. Fraud prevention involves activities designed to prevent fraud before it occurs. Fraud detection activities aim to discover fraud as soon as possible after it has occurred. Fraud response activities, in turn, address the systems and processes that assist an organization to respond appropriately to an alleged fraud when it is detected and include investigations, sanctions and recovery of losses. Fraud prevention, detection, and response are interdependent and mutually reinforcing.

Figure 1: Eight pillars for a robust anti-fraud programme



Source: JIU.

38. While United Nations system organizations have traditionally taken the reactive approach to fraud, focusing on investigations and acting upon fraud cases when they are reported, the review revealed that a number of organizations are shifting slowly towards a more preventive and proactive approach through identifying, assessing and mitigating fraud risks before they become material. As acknowledged by most anti-fraud practitioners, and will be discussed in later chapters, efforts focused on prevention measures are by far the most economical and cost effective in the fight against fraud.

39. **As indicated in figure 1 above, the three categories of anti-fraud activities are supported by eight functional pillars that in their totality constitute a fraud management framework for a robust and effective anti-fraud programme.**

40. The chapters that follow correspond to each of the eight pillars, presenting the concepts involved, current practices in United Nations system organizations,

identifications of gaps and/or good practices, and recommendations as applicable. Specifically they address:

- Chapter IV (Pillar 1) Anti-fraud governance and leadership (fraud policy, roles and responsibilities, anti-fraud culture and fraud awareness)
- Chapter V (Pillar 2) Fraud risk assessments (fraud-specific risk assessments, risks posed by third parties, fraud risk tolerance levels and fraud risk sharing)
- Chapter VI (Pillar 3) Anti-fraud strategies and action plans
- Chapter VII (Pillar 4) Anti-fraud controls (accountability and internal control frameworks, codes of conduct, financial disclosure and declaration of interest programmes, due diligence and screening of staff and third parties, updating of legal instruments for third parties, automation of fraud controls, proactive detection measures, and the role of internal audit in fraud detection and control)
- Chapter VIII (Pillar 5) Fraud complaint mechanisms (whistle-blower policies, whistle-blower hotlines, protection against retaliation, and multiplicity of reporting — centralizes v. decentralized intakes)
- Chapter IX (Pillar 6) Investigations (timeliness, capacity and quality of investigations, investigating third parties, joint investigations, and proactive fraud investigations, case management systems)
- Chapter X (Pillar 7) Disciplinary measures and sanctions (disciplinary process for staff committing fraud, challenges of pursuing perpetrators, vendor sanction regimes, sanctioning of implementing partners, and sharing of information on sanctioning third parties)
- Chapter XI (Pillar 8) Performance reporting and feedback (performance reporting on anti-fraud programmes, lessons learned and feedback, audit and investigation functions interface, anti-fraud cooperation and coordination among entities).

IV. ANTI-FRAUD GOVERNANCE AND LEADERSHIP (PILLAR 1)

41. Member States have clearly raised expectations for high ethical behaviour and zero tolerance to fraud in the United Nations system, as well as for prudent management of programmes through effective corporate governance, including appropriate structures to combat fraud and corruption.

42. As acknowledged in the private and public sectors, the management of fraud is a collective responsibility of all persons employed in an organization and controlling fraud effectively requires the commitment not only of the organization's management and staff, but also of third parties such as vendors, suppliers and implementing partners. The primary responsibility for managing the risk of fraud and setting fraud policies and fraud tolerance levels, however, rests with the organization's top management.

43. It is incumbent upon the executive head and his or her immediate senior managers to ensure that the organization has in place the appropriate corporate governance for controlling fraud and that an ethical culture exists conducive to making the efforts against fraud an integral part of operations at all levels of the organization. Raising fraud awareness and ensuring adherence to the ethical values and norms among staff of United Nations organizations are instrumental to a successful anti-fraud programme.

44. In the JIU fraud survey of staff in the United Nations system, only 55 per cent of the respondents agreed with the statement that "management clearly demonstrates responsibility/commitment for combating fraud"[27] and only 47 per cent agreed with the statement that "management communicates one or more times each year that it does not tolerate fraud".[28] Most respondents indicate that there is room for improvement for management to reinforce the "tone at the top" against fraud.

45. To combat fraud effectively, it is paramount to create a governance environment conducive to such an effort. This entails addressing a number of elements. Three such elements are discussed below: developing and documenting a fraud policy; creating a structure to oversee the anti-fraud effort and assigning roles and responsibilities; and fostering an anti-fraud culture through awareness and training.

A. Fraud policy

46. A fraud policy is the cornerstone of any effective anti-fraud programme. It assists employees and third parties to understand how the organization is addressing fraud and encourage employees at all levels to participate actively in protecting the organization's resources and reputation. It provides the guidelines for decision-making to counter fraud and brings together all relevant policies and procedures that guide the anti-fraud efforts, such as codes of conduct, whistle-blower and anti-retaliation policies, investigation processes, sanctions and disciplinary measures, financial disclosure polices, and internal control and accountability frameworks.

47. As seen in annex I to the present report, a number of United Nations system organizations have in place a stand-alone corporate anti-fraud policy,[29] which provides direction and serves as a repository for the relevant fraud-related policies and procedures.

48. However, in other organizations,[30] anti-fraud-related policies and activities are spread over an array of different rules, regulations, guidelines and administrative issuances, with different owners and different entities responsible for their implementation. This fragmentation often creates duplication of work and

[27] Of the remaining, 20 per cent responded "partially agree", 9 per cent "neither agree nor disagree", 5 per cent "partially disagree", 5 per cent "disagree" and 6 per cent "I don't know".

[28] Of the remaining, 19 per cent responded "partially agree", 10 per cent "neither agree nor disagree", 5 per cent "partially disagree", 12 per cent "disagree" and 8 per cent "I don't know".

[29] See annex I (summary table anti-fraud policies); stand-alone policies of UNHCR, WFP, FAO, WHO, UNOPS, UNDP, UNFPA, UNICEF, ICAO, ILO, UNESCO, UNIDO and WIPO.

[30] The Secretariat of the United Nations, UNEP, UN-Habitat, UNODC, IAEA, ITU, UNWTO, UPU and WMO.

inconsistences, and jeopardizes the effective implementation of the organizations' anti-fraud activities.

49. At the encouragement of internal and external audit bodies, organizations with no stand-alone policies are now in the process of updating their policies to bring them up to best practice standards. The United Nations Secretariat and UNRWA, for example, reported respectively the establishment of task forces to begin the development of more robust anti-fraud policies and strategies. IAEA, however, indicated they do not see a need for a separate anti-fraud policy as they believe existing policies and mechanisms were sufficient in addressing fraud risks.

50. **The review found that, even in organizations that have a corporate stand-alone fraud policy, there is a lack of clear definition of roles, responsibilities and accountabilities or a lack of clear guidance on how to operationalize the policy. For example, in most cases, the owner of the anti-fraud policy is not clearly defined and there are no performance indicators to assess its effective implementation.**

51. The fraud policies reviewed also vary as to their coverage: some policies extend their coverage to third parties, such as vendors, suppliers, and implementing partners, while others do not.[31]

52. In line with good practice, a number of organizations have updated their policies to expand their coverage. One example is the UNDP policy, which stipulates "this policy applies to all activities and operations of UNDP, including any project funded by UNDP, any project implemented by UNDP, and any implementing partner". Similarly, the UNHCR policy states that "this Strategic Framework applies to any fraud or corruption (actual, suspected or attempted) involving UNHCR staff members as well as any party, individual or corporate, having a direct or indirect contractual relationship with UNHCR or that is funded wholly or in part with UNHCR resources".

53. At FAO, the fraud policy: "applies, regardless of their location, to all activities and operations of the Organization, whether funded by Regular Programme or Extra-budgetary Funds; administrative, technical or operational in nature; or implemented by the Organization and/or an implementing partner, including any government agency. This policy applies to all FAO personnel and all contractual arrangements between the Organization and implementing partners, suppliers or other third parties for administrative, technical or operational purposes."[32] The United Nations Educational, Scientific and Cultural Organization (UNESCO) Fraud and Corrupt Practices Prevention Policy explicitly applies to third parties.

54. It was also observed that the process of the adoption of a fraud policy and its legal status varies throughout the system. With the exception of WFP, whose anti-fraud policy was adopted by the organization's legislative body, fraud policies in other organizations are issued variably as an administrative circular or as a directive by senior management.

[31] Please refer to chap. VII, sect. F, for details.

[32] FAO, policy against fraud and other corrupt practices, administrative circular 2015/08 of 12 March 2015.

55. While United Nations system organizations may choose to develop their fraud policy based on particular needs, leading practices suggest that a fraud policy should include at a minimum the following:[33]

- Definition of fraud and an outline of the organization's position on fraud
- Actions constituting fraud
- Management responsibility for prevention and detection of fraud
- Unit/person(s) responsible for administration of the policy
- Commitment to investigate and prosecute fraud or pursue other effective remedies
- Employee and third party responsibilities relating to the prevention and detection of fraud and procedures on how fraud is to be reported
- Consequences of acting fraudulently
- Assurance that allegations and investigations will be treated confidentially
- Directions as to how allegations/incidents of fraud are to be managed
- Advice on where further information can be found (i.e., other relevant policies and guidance such as code of conduct, whistle-blower and anti-retaliation policies, disclosure policies etc.)

56. The implementation of the following recommendation is expected to enhance the effective delivery of organization's anti-fraud programme, based on good practices.

Recommendation 2

The executive heads of the United Nations system organizations, if they have not already done so, shall develop a corporate anti-fraud policy for their respective organizations or update an existing one, taking into account leading practices in the public and private sectors. The policy should be presented to the legislative and governing bodies for information, adoption and/or endorsement and should be reviewed and updated regularly.

B. Assigning roles and responsibilities

57. Good practice dictates that effective corporate anti-fraud programmes assign a clear owner of the organization's fraud policy and set out the roles and responsibilities of the different entities and those fulfilling certain functions, including of management, finance departments, investigators, auditors, legal departments, human resources departments, programme management and staff at large.

[33] Adapted from ACFE, *Occupational Fraud in Government* and Australia, *Commonwealth Fraud Control Guidelines* (2011).

58. In addition to assigning a principal owner of the fraud policy, anti-fraud responsibilities should cascade down along the lines of delegation of authority from senior management to middle management and staff members. While a fraud policy document at the headquarters level may not provide details and guidance on the anti-fraud activity at each of the lower levels, it is the responsibility of the respective managers to address anti-fraud activities based on the fraud risks identified through specific risk assessments of their programmes and activities. As indicated in chapter V (Fraud risk assessments), fraud risks vary depending on the type of operation and particular function.

59. The review revealed that most organizations fail to present a clear picture of the anti-fraud roles and responsibilities of management and staff. Most of the fraud policies reviewed are vague in this respect, with some, for example, stating that managers are responsible for certain aspects of the policy without specifying which aspects. Others are silent on who holds the overall responsibility for implementing anti-fraud activities. According to the responses provided to the JIU questionnaire, many organizations view oversight/investigation offices as the leading anti-fraud entities within their organization. Other organizations have no lead entity, relying instead on a collaborative effort by several entities, such as investigations, human resources and management departments, ethics offices etc., on the basis of their respective responsibilities. Finally, some organizations indicated that (senior) management, including executive heads, have the leading role.

60. The policies of some organizations, however, are more specific. For instance, the WHO policy clearly states that the Director-General, as the head of the organization, has overall responsibility for the prevention and detection of fraud, misappropriations and other inappropriate conduct. The UNHCR anti-fraud policy outlines specifically the responsibilities of staff, managers and implementing partners and other contractual parties and includes, in an annex, a reference matrix that designates "focal point" departments for various sensitive and other areas that fall under the fraud policy.[34] The UNESCO anti-fraud policy describes the specific roles, authorities and accountabilities in matters relating to fraud. It states that "The Director-General has overall responsibility for implementing measures to prevent fraud and corrupt practices",[35] but also clarifies that every staff member has a responsibility in respect of fraud prevention and detection, in particular staff member having delegated authorities from the Director-General for the management of human resources and utilization of the financial and material resources of the organization. The policy describes the different structures within the organization that have specific authorities in the prevention, detection or investigation of fraud and corrupt practices (i.e. the Internal Oversight Service, the Ethics Office, the Bureau of Human Resources Management and the Office of International Standards and Legal Affairs).

61. In several United Nations system organizations, no senior manager is assigned to lead the implementation of the organization's fraud policy and programme. Following leading practices and in view of the importance of leadership and setting

[34] UNHCR, *Strategic Framework for the Prevention of Fraud and Corruption* (2013), sect. 6 and annex 2.

[35] UNESCO, Administrative Manual (2012), item 3.14 "Prevention of Fraud and Corrupt Practices", para. 4.2.

the "tone at the top" for a strong stand against fraud in the organization, the designation of an anti-fraud entity (senior person or team) as the "business process owner" of all fraud-related activities is strongly advised.

62. **A number of United Nations system organizations seem to believe, wrongly, that the internal oversight offices should play the leading role in managing anti-fraud activities. It is important to note that the leading anti-fraud entity should be in the management function and not be located in the internal oversight office, as this office needs to maintain and preserve its independence to conduct its oversight responsibilities.**

63. The implementation of the following recommendation is expected to enhance the effective implementation of organization's anti-fraud programme and assure clear responsibilities and accountability in this regard.

Recommendation 3

The executive heads of the United Nations system organizations should take expeditious action to designate an overall corporate manager or entity at senior level to be the custodian of the anti-fraud policy and be responsible for the implementation, monitoring and periodic review of the policy.

C. Anti-fraud culture and fraud awareness

64. Fraud awareness-raising measures comprise specific actions taken in order to: (a) convey to staff and other stakeholders the importance that the organization attaches to the fight against fraud and the support of ethical culture; (b) educate stakeholders about the mechanisms available to them to report potential fraud; and (c) deter potential fraudsters by increasing their awareness of becoming exposed.

65. As discussed, senior management plays a vital role in raising fraud awareness and adherence to the values and norms among the staff of United Nations system organizations. It is senior management's responsibility to set the "tone at the top" by behaving ethically and openly communicating expectations to the staff, creating a positive workplace environment, hiring and promoting employees who are competent and have the right work ethic, implementing a code of conduct, ensuring that fraud controls are implemented and taking disciplinary actions when necessary. As noted by an audit and oversight advisory committee of one of the organizations reviewed, strong communications relating to fraud prevention and mitigation must be issued from the highest level in order to enforce the zero tolerance policy that the organization advocates.[36]

66. Different approaches and measures are used in the United Nations system to raise fraud awareness. In addition to anti-fraud training (as discussed below), such measures include: holding "anti-fraud days" and other public events, and communication activities, such as the publication of brochures, pamphlets and articles on internal and external websites, interviews, question and answer sections

[36] See EC/66/SC/CRP.26, Report of the Independent Audit and Oversight Committee, 2014-2015, para. 35.

etc. At the International Labour Organization (ILO), for instance, five presentations on anti-fraud awareness and prevention were delivered in their offices in 2014.[37] Good practice calls for annual refresher training for all staff to stay abreast of fraud risks independent of a staff member's seniority. For senior management, best practice is to communicate with specific messages of ethics and integrity at least once a year.

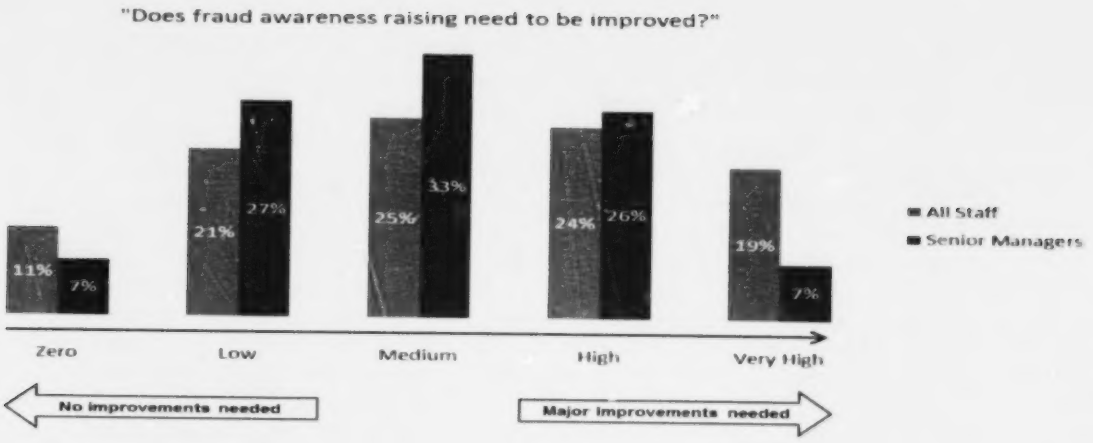
67. Finally, multi-element communication and fraud awareness-raising campaigns organized by cross-departmental initiatives (human resources departments, Ethics Offices, auditors etc.) can be particularly effective. For example, UNHCR plans to use the annual International Anti-Corruption Day to hold a fraud awareness week organized jointly by the Ethics and Controller's Offices. The UNOPS Internal Audit and Investigations Group and Ethics Office developed a workshop on standards of conduct together, training personnel to spot potential issues and know where to report concerns or suspicions. IAEA provides training for members of its staff council on misconduct and on the whistle-blower policy. The UNICEF Executive Director announced in a 2015 communiqué to all staff that he had taken the updated mandatory ethics course and expects all staff to do the same.[38] WIPO distributes to all staff an annual circular on disciplinary measures applied in the organization, as a means of raising awareness and deterring further fraud. Similarly, at UNFPA, the Deputy Executive Director (Management) sends regularly to all staff a summary of disciplinary measures taken when there is a sufficiently high number of cases that have an adverse impact on the organization. At FAO, the Office of the Inspector General (OIG) has prepared flyers and posters aimed at raising awareness about fraud. In addition, OIG regularly takes advantage of its investigative missions to make presentations about its activities and raise awareness about reporting mechanisms and other relevant information. OIG has also conducted stand-alone missions and briefings for internal stakeholders and other procurement personnel regarding sanctionable actions and the vendor sanctions procedures.

68. Notwithstanding the ongoing efforts of some organizations to raise fraud awareness, many interviewees indicated that much more can be done in this area. Also, the majority of respondents to the JIU fraud survey highlighted fraud awareness-raising as one of the areas in need of major improvements. On a scale from 1 to 5 (with 1 being "no improvement needed" and 5 being "major improvements needed), the majority of staff saw a need for improvement (see figure 2 below).

[37] ILO, report of the Chief Internal Auditor for the year ended 31 December 2014, GB.323/PFA/8, para. 11.

[38] UNICEF, message from the Executive Director on the online course "Ethics and Integrity at UNICEF", 24 June 2015.

Figure 2: Fraud awareness



Source: JIU fraud survey.

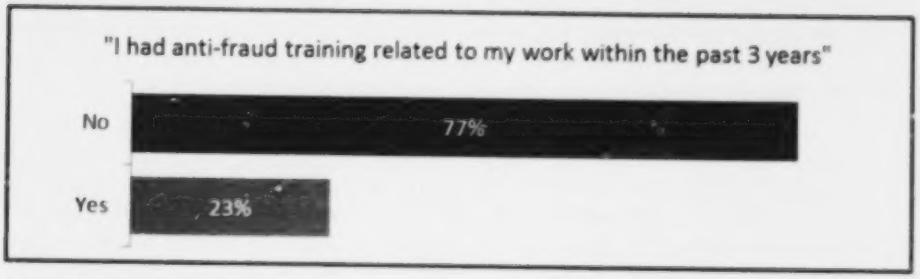
69. **The Inspectors reiterate the call made in previous JIU reports[39] for organizations to institute fraud awareness initiatives, to address fraud prevention and detection at all levels of the organization.**

Anti-fraud training

70. Anti-fraud training is a major component of an organization's fraud awareness and the development of an anti-fraud culture. It provides staff with the know-how to effectively prevent and detect fraud, in particular in fraud-prone areas. Despite the importance of anti-fraud training, according to the JIU fraud survey of the United Nations system, more than 77 per cent of staff surveyed has not had any fraud-related training in their work environment in recent years (see figure 3 below).

[39] JIU in its report on oversight Lacunae in the United Nations System (JIU/REP/2006/2), recommendation 15, recommended that "The legislative bodies in each organization should direct their respective executive heads to put forward proposals for [...] mandatory integrity and ethics training for all staff, particularly newly recruited staff". In its report on ethics in the United Nations system (JIU/REP/2010/3), JIU suggested a number of standards for Ethics Office responsibilities, including, "Ethics office takes the lead role in developing mandatory training programmes (initial and refresher) and workshops for all staff of the organization" and, in its report on review of the management of implementing partners in United Nations system organizations (JIU/REP/2013/4), recommendation 8, JIU stated: "The executive heads of United Nations system organizations should institute training in fraud awareness and prevention, with emphasis on fraud related to third parties, for staff engaged with Implementing Partners (and especially staff in country offices)."

Figure 3: Anti-fraud training



Source: JIU fraud survey.

71. Most United Nations system organizations have in place general and mandatory ethics training for their staff. For example, UNHCR offers annual refresher courses on their code of conduct to all offices. However, in general, most ethics training courses in the United Nations system do a cursory review of fraud-related issues and do not include specific information on fraud prevention, detection and response. A few organizations have started to do so. For example, UNICEF has a module on "prevention of fraud and whistle-blower protection" included in its "Ethics Essentials" course; the UNRWA ethics programme highlights a number of fraud "red flags" and explains staff requirements to prevent and detect fraud; and UNFPA ethics training elaborates on specific fraud elements. FAO plans to include fraud awareness in its corporate integrity training. At the United Nations Secretariat, the Ethics Office, in conjunction with OIOS, is designing a mandatory e-learning programme on fraud awareness and prevention. This ethics training module is intended to be a basic prevention module on topics such as identifying, detecting and speaking out against fraud and corruption, and it will also deal with any ensuing retaliation concerns, as well as reinforcing compliance by all United Nations staff with staff regulations and rules and standards of conduct.

72. While some ethics training is still delivered in face-to-face sessions, in recent years e-learning courses have become prevalent and are increasingly mandatory for all staff.[40] Hence, they reach a wide group of participants with their topics covering ethical behaviour, rules, regulations, integrity and proper conduct. Some ethics courses target specific groups of staff, such as procurement, human resources, accounting and finance staff etc., who inherently are more prone to irregularities.[41]

73. As discussed, this review has shown that, while some ethics courses include anti-fraud topics, such as the above-mentioned examples, the majority do not cover the subject adequately. **It is recommended that organizations consider including**

[40] UNFPA, WFP, FAO, UNDP and UNICEF, for instance, have launched their new online, mandatory ethics courses in the past year or are in the progress of enrolling them.

[41] The Secretariat of the United Nations provides an "Ethics and Integrity in Procurement" course for staff of the UN procurement division (UNPD) and others with procurement-related duties. The UNDP Ethics Office provides sessions for human resources practitioners and briefings for senior leadership. UNICEF made an ethics awareness course mandatory for staff at level P5 and above, as well as all deputy representatives, and chiefs of operation and zone offices, and also offers ethics briefings for human resource staff moving to country offices. IAEA provides mandatory ethics training for procurement and finance officers.

in their ethics and integrity training, elements or modules on fraud prevention and detection, such as examples of unethical/fraudulent conduct, information on the obligation to report misconduct and fraud, the organization's protection against retaliation policies and procedures, and other prevention and detection measures.

74. A number of organizations offer dedicated anti-fraud training separate from the ethics courses. UNIDO provides a mandatory, web-based "introduction to fraud awareness" addressed to all staff. It also has a special introductory online course on its fraud policy, as well as a course that teaches staff how to detect and address anomalies in documents. At FAO, the procurement unit delivers a dedicated module to fraud prevention and detection training and its OIG is developing a strategy for conducting bi-quarterly anti-fraud training via video conference for country/regional offices. In 2015, WFP launched a mandatory online anti-fraud course for staff at large,[42] and it also offers fraud prevention training at management's request. UNDP investigators occasionally provide specific anti-fraud training to country/regional offices when on mission. As a measure of good practice, UNICEF has made participation in fraud awareness-related training mandatory for senior staff (P5 and above). It has also introduced a training programme for field-based Ethics Dialogue Facilitators, including a module on fraud prevention and whistle-blower protection. At the United Nations Secretariat, a course by the Chartered Institute of Procurement and Supply (CIPS) procurement training deals with fraud awareness, and procurement staff of the Secretariat and other organizations, such as the International Telecommunication Union (ITU), take the course voluntarily or as part of their CIPS certification. UNHCR incorporated fraud elements into the training module for representatives and finance staff in the field. UNFPA holds specific anti-fraud courses for the Procurement Services function as part of the CIPS training programme.

75. Considering the commonalties that exist among the training offered by organizations across the system, **it is recommended that the executive heads of United Nations system organizations explore the sharing of existing training material and consider the joint development of anti-fraud e-training courses through the CEB/HLCM and its networks, the Panel of Ethics Offices, the United Nations Representatives of Investigative Services (UN-RIS), and other formats, as applicable.**

76. Notwithstanding the above initiatives of dedicated anti-fraud training, the JIU fraud survey respondents highlighted anti-fraud training as one of the areas that needed much improvement in combating fraud. While a number of organizations have made commendable efforts to strengthen anti-fraud awareness and training, more needs to be done to expand the content, quantity and reach of the course material. As discussed, this includes incorporating anti-fraud modules in existing training material and also providing anti-fraud dedicated training, particularly for managers and staff working in functional areas most prone to fraud. Whether or not

[42] The WFP online course "Anti-fraud and Anti-Corruption and Protection from Sexual Exploitation and Abuse", launched 2015, is mandatory for all staff. Apart from that, face-to-face fraud prevention training is provided (WFP, Annual Report of the Inspector General for 2014, WFP/EB.A/2015/6-F/1, para. 27, and Add.1, para. 11). In 2013, UNIDO introduced mandatory online training regarding the UNIDO Policy on Fraud Awareness and Prevention.

the training courses should be mandatory depends on the risk profile of the organization and level of fraud mitigation levels required.

77. Finally, consideration should be given to providing anti-fraud training to third parties and other stakeholders responsible for fraud controls.

78. The implementation of the following recommendation is expected to enhance the effectiveness and efficiency of the organization's anti-fraud programme through improved anti-fraud training and fraud awareness of staff and managers.

Recommendation 4

On the basis of a comprehensive needs assessment, the executive heads of the United Nations system organizations should establish a dedicated anti-fraud training and fraud awareness strategy for all members of the organization. At a minimum, anti-fraud training should be mandatory for staff in functional areas most prone to fraud and staff operating in fragile and high-risk field environments.

V. FRAUD RISK ASSESSMENTS (PILLAR 2)

79. Fraud risk assessments are an essential component of and a prerequisite to an effective anti-fraud programme. They assist in systematically identifying where and how fraud may occur, so that proper controls to mitigate fraud-related risks may be devised. Fraud risk assessment includes the following elements: identifying inherent fraud risk factors and potential fraud schemes; assessing the likelihood and impact of the risks; determining fraud risk tolerance levels; mapping the suitability of existing fraud controls to potential fraud schemes and prioritizing residual fraud risks; documenting key findings and conclusions; and testing effectiveness of fraud controls.[43]

80. In 2013, the Committee of the Sponsoring Organizations of the Treadway Commission (COSO) issued an updated framework for the design, implementation and conduct of systems of internal controls and the assessment of their effectiveness. Under this framework, which came into effect in December 2014, fraud risk assessments are now given specific consideration in the context of the enterprise risk management system of an organization. Principle 8 (a new principle) of the COSO framework specifically requires that, "the organization considers the potential for fraud in assessing risks to the achievement of objectives".

81. While every type of organization is prone to fraud, many United Nations system organizations are more exposed than others because they often operate in high-risk environments, such as post-conflict, conflict and humanitarian emergency settings. Depending on the organization's structure, programmes and business model, comprehensive fraud risk assessments allow management to determine the

[43] International Professional Practices Framework, *Internal Auditing and Fraud*, Practice Guide, and United States Government Accountability Office, *A Framework for Managing Fraud Risks in Federal Programs* (2015).

organization's specific fraud risk profile[44] by identifying and assessing internal and external fraud risks and associated risk tolerance levels, and subsequently devise risk mitigation approaches that include proportionate resources to address the levels of fraud.

82. Leading practices call for fraud risk assessments to be conducted at multiple organizational levels, from headquarters to regional and field offices, and should cascade down to the programme, project and transaction levels, including to third parties (contractors, vendors and implementing partners). As also noted by the BOA, detailed fraud risks need to be assessed for each business area and process, including, for example, cash payments, cash receipts, purchasing, partner expenditures, inventory, payroll etc. This has to be aligned with and benchmarked against the existing system of internal control and the business environment of the entity.[45]

A. Status of fraud-specific risk assessments

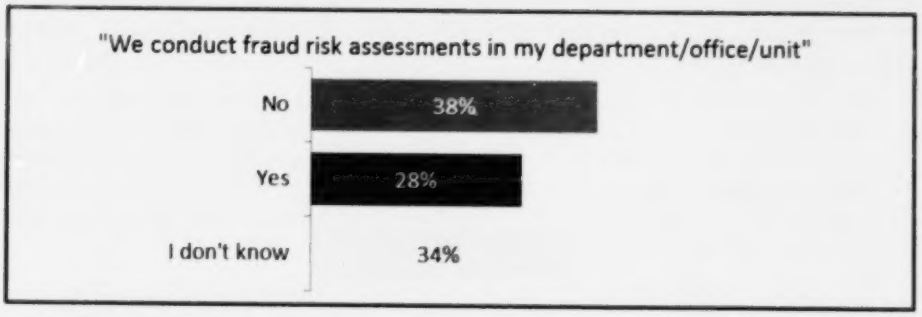
83. **The review found that, with a few exceptions, most United Nations system organizations do not conduct systematic fraud risk assessments or consider fraud to be a corporate risk.** For example, only 28 per cent of respondents to the JIU fraud survey indicated that they conduct fraud risk assessments in their department/office/unit (see Figure 4 below). However, the situation may be worse, as the above survey results do not reflect what was collected as additional evidence from the answers to the separate questionnaires sent to organizations and the results of subsequent person-to-person interviews. The evidence provided shows that only two organizations (UNHCR and WIPO)[46] have conducted specific corporate fraud risk assessments. These assessments were conducted for the first time in the past two years. This is indicative of the United Nations system's low level of awareness regarding the impact fraud has on an organization's operations and the importance of fraud risk assessments in realizing the extent and level of fraud.

[44] United States Government Accountability Office, *A Framework for Managing Fraud Risks in Federal Programs* (2015).

[45] A/70/322, para. 48.

[46] UNRWA conducted a risk analysis of *Preventing corruption in UNRWA* in 2012; UNOPS is planning to conduct a similar exercise.

Figure 4: Fraud risk assessments



Source: JIU fraud survey.

84. Also, in organizations that have in place a corporate enterprise risk management (ERM) system, it is often not clear if fraud risks are being assessed in the context of their overall ERM processes. In some organizations, such as UNICEF, UNESCO, WHO and UNFPA, fraud is listed as one of the major corporate risks and they reported that fraud receives due consideration. Others, such as IAEA, UNDP, the World Meteorological Organization (WMO), the Universal Postal Union (UPU) and the International Civil Aviation Organization (ICAO), reported that the risk of fraud is a consideration within the corporate risk management processes and that they did not envision the need for a specific risk exercise to address fraud. UNDP, however, did indicate that, as part of forthcoming policy revisions, it might consider the need for targeted fraud risk assessments in areas where the specific risks of fraud are considered high.

85. At WFP, managers assess risks that reportedly include fraud risk as part of ERM.[47] Preparation of a risk register is included in the annual performance planning and a risk assessment is conducted twice yearly. At FAO, there is no specific fraud risk assessment conducted as part of its current ERM activities. FAO considers that the hazard and control risks that create a vulnerability to fraud also create vulnerabilities to other financial, programmatic and reputational risks. Therefore, FAO reported that managers assess fraud risks while assessing the broader risks to their area of responsibility.

86. Annex III to the present report provides an overview on how fraud risks are addressed in risk assessments conducted by organizations, including in the context of their ERM processes.

87. WHO initiated the roll-out of its organization-wide risk management approach in 2014 and reported that fraud risks are specifically considered as part of the exercise. The Office of Compliance, Risk Management and Ethics developed a corporate risk management policy, adopted in November 2015, and is currently in the process of analysing risks, including the respective risk tolerance levels.

88. At the urging of BOA, UNHCR has taken a lead in combating fraud by initiating a fraud prevention project that consists of a dedicated working group drawing on the knowledge of managers across business areas. Internal and external

[47] Enterprise Risk Management Policy, WFP/EB.A/2015/5-B (2015).

fraud risks have been identified through a series of workshops held in early 2015. Those risks are now being assessed against the existing control framework to identify any gaps in mitigating controls and identifying the residual risk of fraud in UNHCR operations.

89. In UNICEF, offices are required to perform risk self-assessments and they indicated fraud is a risk area that they assess. These self-assessments are currently performed once every two to four years, with plans to conduct them annually once risk assessment software, currently being developed, is implemented. UNFPA reported that strategic and operational risk self-assessments are conducted annually by country offices, which cover fraud risks.

90. At the United Nations Secretariat, an enterprise risk assessment was conducted in 2014 under the auspices of the Management Committee to identify, evaluate and prioritize the top strategic risks for the organization and related managerial responses. However, fraud is not considered a corporate risk and no specific fraud risk assessments are conducted.

91. While the above overview shows some steps have been taken in the right direction, more needs to be done. To reiterate, fraud risk assessments are essential for an effective anti-fraud programme, as they allow the identification and definition of the fraud risk exposure of the organization. Fraud risks are not limited to certain functions or activities of the organization but are cross-cutting. They also evolve over time, and hence there is a need for periodic conduct or review of such assessments.

92. Fraud-related risk assessments require specific expertise and skills. Accordingly, the organization's anti-fraud training should include such training for those involved in fraud risk management, including programme managers, risk officers, and auditors and investigators.

93. The implementation of the following recommendation is expected to enhance the mitigation of fraud risks as well as the effective delivery of organization's anti-fraud programme.

Recommendation 5

The executive heads of the United Nations system organizations should, if they have not already done so, conduct a comprehensive corporate fraud risk assessment, as an integral part of their enterprise risk management system or as a separate exercise, addressing fraud risks at all levels of their respective organization, including headquarters and field offices, as well as internal and external fraud risks. Such assessments shall be conducted at least biennially at the corporate level, and more frequently, based on need, at the operational level.

Fraud risk assessments by audit offices

94. While the overall enterprise risk management (ERM) function of the organization is the responsibility of management, fraud and other risks are also assessed by internal audit offices when they are developing their annual workplans

and audit engagements. However, it is important to note that internal audit's risk responsibilities differ from those of the ERM function. Internal auditor's role is to provide overall assurance on risk management and advise the organization on risk issues, but not be a principle in designing and/or implementing the ERM system of the organization, the risk registers, or risk tolerance levels. The review found that while internal auditors take into account the risks identified by the ERM process, they mostly rely on their own risk assessments pertaining to the specific audit plans and engagements. **Reliance of the ERM function on the internal audit's risk assessments, or vice versa, is not a frequent occurrence in the organizations reviewed for this report. There is need for closer coordination and cross-feeding between the two activities as they complement each other.**

95. At the WFP Office of Internal Audit, fraud risk elements are included in the annual risk assessment undertaken by the Office of Internal Audit to inform the audit work plans. This includes the use of such risk indicators as a corruption perception index for the areas of operations, the business unit's responses to annual assurance statements (which feed into the WFP Statement on Internal Control) and results of previous audit and evaluation reports. At the engagement level, the fraud risk is considered in more detail for each process area.

96. Similarly, in UNFPA, the Office of Audit and Investigation Services takes into account fraud risks in its annual audit risk assessments and incorporates the World Bank corruption index indicators for field operations, as well as fraud-related leads communicated by the investigation function.

97. At FAO, the Risk Based Audit Plan of the Office of the Inspector-General considers fraud risk along with other types of risks in order to assign an overall risk rating to each auditable entity in the audit universe. Fraud risk usually has more weight in the overall assessment in areas which are traditionally prone to fraud, based on actual reported cases (e.g., procurement, staff entitlements). The Office of Internal Oversight Services of WHO requests that auditees complete a fraud risk self-assessment questionnaire as part of the audit planning phase, in advance of a field visit, or conduct detailed testing to garner the views of the head of the country office.

98. A number of other oversight entities such as the Office of Audit and Investigation of UNDP and OIOS of the United Nations Secretariat have, on a pilot basis, initiated proactive fraud risk reviews or proactive investigations (see also chapter IX below in this respect).

Assessment of fraud risks posed by third parties

99. As discussed, many United Nations system organizations are exposed to high risks owing to their dependency on third parties (i.e., vendors, suppliers and implementing partners) for the delivery of their programmes, especially when operating in fragile environments and remote project sites.

100. The review found that the challenges of working with third parties in high-risk environments are not fully appreciated by all stakeholders. In most cases, the existing controls, accountability and management arrangements do not match the high risk of fraud and corruption found in such environments.

101. In this respect, the Inspectors **refer to the relevant recommendations of the JIU report on the management of implementing partners (JIU/REP/2013/4).** As indicated in the report, the up-front implementing partners' assessments and due diligence processes are of particular importance so as to determine the capacity and potential weaknesses and risks of an implementing partner, including fraud risks. These assessments provide a basis for the concomitant mitigation of those (fraud) risks through establishment of appropriate control and risk mitigation measures, such as monitoring, verification, reporting and other practices subject to the risk levels assessed.

B. Fraud risk tolerance levels

102. Adopting a zero tolerance policy to fraud is viewed as a signal of a clear resolve to fully investigate and sanction all cases of fraud no matter how minor.[48] The benefits of such a policy include the articulation of the tone from the top against fraud, the establishment of a deterrent effect and the communication of the organization's resolve in fighting fraud by all means. However, implementing such a policy in certain environments may be impractical or cost prohibitive.

103. Zero fraud tolerance in a strict sense may imply the need for a full range of fraud controls in place to prevent and detect all fraudulent activities. Fraud risk controls, however, come with costs to the organizations, in terms of financial, human and other resources. Fraud risks may vary depending on a number of factors, such as the type of activities and the operating environment. In unstable and emergency settings, where the United Nations system often operates, risks may be particularly high. In these situations, implementing an absolute zero fraud tolerance approach may not be practical in view of effectiveness and cost efficiency. It may also impede delivery of the core mandate, for example when swift and rapid action is required, which may not be possible if the standard control and verification procedures prove to be cumbersome and time consuming.

104. International organizations, including some in the United Nations system, acknowledge these operational realities and constraints and have started to address fraud tolerance in the context of fraud risk management. While the approaches differ from one organization to another, risk tolerance reflects the organization's willingness to accept a higher level of fraud risks and this may vary depending on the circumstances of the particular program or activity.

105. In some organizations declared risk appetite levels provide guidance for appropriate risk tolerance levels in certain environments. WIPO has established the Risk Appetite Statement, and risk appetite is incorporated into the WIPO Risk Management Policy of 2014. WIPO defines its risk appetite in terms of: (a) operational risks (including fraud); (b) financial risks; (c) strategic risks; and (d) reputational impact. In that light, the organization's risk appetite approach is: (a) risks with a small impact are accepted where the likelihood of the risk event is assessed as moderate, low or minimal; (b) risks with a noticeable impact are accepted where the likelihood of the risk event is assessed as low or minimal; and (c) risks with a critical impact are accepted only where the likelihood of the risk

[48] Newborn and Jones 2007. See www.U4.org.

event is minimal. Any risks in excess of the WIPO risk appetite are assessed by programme managers and/or the WIPO risk committee, taking into account risk tolerances. Such risks are accepted after ensuring that the mitigation measures in place are suitable and appropriate.

106. At WFP, the Enterprise Risk Management Strategy of May 2015 includes a risk appetite statement that specifically mentions fraud risk: "We accept that our operating environment heightens exposure to the risk of fraud, corruption and collusive practices. Fraudulent, corrupt, and collusive practices and misappropriation of resources are contrary to WFP's core values and are not accepted by the organization. WFP is committed to preventing such practices and to taking mitigating action where they are found to occur."[49] WFP's ERM policy states: "WFP's risk appetite provides the basis for setting acceptable levels of risk tolerance in relation to each of its objectives ... The risk appetite of WFP will guide the decisions of managers, who have the necessary authority and are empowered to take decisions in line with the overall risk management framework."[50]

107. Other United Nations system organizations stated that they have adopted and strictly adhere to a policy of zero tolerance to fraud. UNDP reported zero tolerance for fraud when considering the investment in compensating controls. Similarly, UNFPA strictly applies the principle of zero tolerance to misconduct as per its oversight policy. UNESCO has formally adopted a zero tolerance approach to fraud as set forth in its Fraud and Corrupt Practices Prevention Policy. However, FAO reported that in its multi-stakeholder environment, a quantified risk tolerance for fraud is not practical.

108. While trying to achieve zero fraud should be the ultimate goal and the right approach in dealing with fraud, there is merit in establishing in an efficient and cost-effective manner a risk appetite which would help organizations to adopt consistent risk mitigation and response measures based on acceptable levels of risk. As discussed above, the acceptable risk levels and associated controls may vary depending on the type of activity and the operational environments. In certain unstable and fragile settings, different levels of fraud risks may be considered, as a strict zero tolerance approach would not be feasible in view of the extent and resources required for such mitigation measures. This does not mean that no fraud controls should be in place, but rather proportionate controls should be envisioned based on acceptable risks dictated by the environment. In this context, organizations should define and document risk tolerances levels that are specific and measurable.

109. Zero tolerance to fraud should not translate to zero appetite for fraud risk. The risk of fraud can never be eliminated or reduced to zero; rather, it can be mitigated effectively by having in place a robust anti-fraud risk management programme. Putting in place such a programme and taking swift action when fraud is detected is in line with the meaning and the intent of 'zero tolerance to fraud'.

110. **It is recommended that the executive heads of United Nations system organizations operating in decentralized and/or fragile risk environments consider defining operational risk appetite levels based on specific fraud risk assessments and proportionate mitigation measures. The risk appetite**

[49] Enterprise Risk Management Policy, WFP/EB.A/2015/5-B, annex, para. 8.
[50] Ibid., paras. 35-37.

statements should be submitted to the organizations' legislative and governing bodies, as necessary, for information and/or endorsement and be shared with major contributors for their information.

C. Fraud risk sharing

111. The sharing of fraud risks among donors, United Nations system organizations, and programme recipients, is an area that needs to be further explored among the various stakeholders. Many interviewees indicated that sharing of risks is a prudent approach in producing a more conducive environment for programme implementation. Yet, opinions vary widely on how and if risks can be shared between donors and organizations.

112. The current practice in most cases is that when donors transfer funds to the United Nations system, they expect the organizations to absorb most, if not all risks associated with the implementation of the programme, inclusive of fraud risks. Most donors demand a zero tolerance policy on fraud which in many cases also translates to zero tolerance on fraud losses. This, however, is more problematic when the United Nations system implements programmes in high-risk settings, such as emergencies, humanitarian crises and conflict and post-conflict environments. As discussed in the previous section, in such settings it may not be possible to establish an ironclad level of fraud controls as this may not be practical in terms of cost and effective delivery of core mandates. In other words, implementing a 'zero tolerance to fraud' policy by the organization and having in place fraud preventing measures does not necessarily prevent loses from occurring in all circumstances.

113. At issue is not only the adequacy and suitability of an organizations' existing anti-fraud policies, but also prioritization and sharing of residual[51] fraud risks among all the stakeholders. Demands from donors for return of funding related to fraud losses (non-recoverable) appear to have no merit when organizations have done their due diligence and have in place expected risk mitigations measures. A related issue is whether transfer of financial liability is feasible when organizations are voluntarily funded. Recovery of fraud losses demanded by a particular donor for a specific project/program would necessitate the organization using central funding which in most cases comprise funds from other donors.

114. It would be useful for both donors and the United Nations system organizations to allow for entering into discussions and negotiations on the acceptable levels of fraud risks, and possible risk-sharing arrangements. Discussions should include defining the risk tolerance levels that may be acceptable, depending on the operational environments, as well as the resources available for adequate mitigation measures. This will require a commitment on the part of organizations to be more forthcoming in discussing with donors internal risk management procedures and making available information on the risks and challenges they are facing. It will also require willingness on the part of the donors to agree on specific acceptable financial risk levels or on directly costing the fraud related risks.

[51] Residual risks are the risks that remain after the organization considers the extent to which existing control activities mitigate the likelihood and impact of inherent risks.

115. Such risk sharing is good practice in the private and public sectors around the world that operate in adverse environments and in similar settings. United Nations system organizations face a precarious position of having to absorb all the risks and be the only ones responsible and liable in case of losses in high-risk environments.

116. **It is recommended that United Nations system organizations explore opportunities of discussing and negotiating risk tolerance and risk-sharing arrangements with donors for high risk programmes and projects. Donor agreements should reflect these arrangements and proportionate resources to mitigate such risks should be identified.**

VI. ANTI-FRAUD STRATEGIES AND ACTION PLANS (PILLAR 3)

117. The review revealed that, while a number of United Nations system organizations have updated or developed new policies addressing the management of fraud risk (see chapter IV above), only a few have gone further to adopt corporate anti-fraud strategies and action plans to operationalize the policies and integrate them with existing corporate risk management systems, strategic plans or operational activities. As a result, most organizations have a fragmented, often ad hoc and incoherent approach to combating fraud. Furthermore, organizations that are taking steps to address fraud in a more systematic and strategic manner have done so only recently and most organizations reported the status of their efforts as "work in progress", making it difficult for this review to assess implementation and degree of success.

118. Anti-fraud strategies need to be commensurate with the assessed fraud risks, as not all programmes and activities face the same level of risks. Such strategies can help achieve a cost-effective approach to combating fraud by focusing on areas where efforts may have the greatest impact. Furthermore, a comprehensive strategic approach may help the organization make a strong case for identifying the right level of resources needed for the anti-fraud effort.

119. The lack of anti-fraud strategies and action plans is a subject of concern to a number of managers and staff who were interviewed. This is especially the case in organizations with a decentralized structure and delegation of authority to field offices where, in most cases, the risk of fraud is often higher. The majority of interviewees see the need for having an anti-fraud strategy that is aligned with the overall organizational strategy in achieving corporate objectives.

120. As indicated in a recent report by BOA,[52] 13 entities subject to the oversight of BOA did not have adequate anti-fraud strategies. One positive example is UNOPS, which had established an integrated counter-fraud strategy that focused on all types of fraud (both internal and external).[53] Another good example is UNHCR, which, as discussed, has embarked on a fraud prevention project, and in that context it has updated its corporate fraud policy and is developing an anti-fraud strategy and programme.

[52] A/70/322, para. 45.
[53] Ibid., para. 45.

121. Good practice in other international organizations suggest that anti-fraud strategies and action plans should address prevention, detection, and response measures at all levels of an organization and should include at a minimum the following:[54]

- A summary of the identified internal and external fraud risks or vulnerabilities associated with the organization's activities or functions
- The treatment strategies or controls (including policies, governance and other structures, and procedures) put in place to mitigate the identified risks or vulnerabilities
- Information about implementation, such as identifying functions and/or staff responsible for implementation
- Senior management's monitoring of performance and review of plans and measures and periodic reporting on implementation of the fraud policy
- Arrangements, channels and processes for staff, contractors or third parties (vendors, suppliers, implementing partners) to report fraud or suspected fraud
- Strategies to ensure the organization meets its fraud training needs
- Developing a real anti-fraud culture and awareness
- Mechanisms for collecting, analysing and reporting the number and nature of incidents of fraud or alleged fraud within or against the entity
- Protocols setting out how the entity will handle allegations or suspicions of fraud, including assessment of allegations, establishment of investigations and options for resolution of incidents (such as referral to national authorities and when and how to initiate a recovery action).

122. As discussed, anti-fraud strategies should be based on acceptable risk levels, with due regard to the proportionality of anti-fraud measures and assessment of costs and benefits of the organization concerned.

123. The implementation of the following recommendation is expected to enhance effective and efficient delivery of programmes through minimizing exposure to fraud.

Recommendation 6

The executive heads of the United Nations system organizations, if they have not already done so, should develop organization-specific comprehensive anti-fraud strategies and action plans for implementing their respective fraud policies. Such anti-fraud strategies should be based on the organization's corporate fraud risk assessments and shall be an integral part of the overall organizational strategies and operational objectives. Based on the level of fraud risk, proportionate resources should be dedicated to operationalize the strategies and action plans.

[54] Adapted from "*Commonwealth Fraud Control Framework* (2014)" Australia; and BOA suggestions, (A/69/5, Vol. I), para. 158.

VII. ANTI-FRAUD CONTROLS (PILLAR 4)

124. Internal control and compliance issues have been repeatedly identified as areas of high concern in various audit reports in many United Nations system organizations. In particular, internal controls in areas and activities more prone to fraud such as procurement, implementing partners, human resources and recruitment, project management, entitlements, and management of assets, have been found deficient by internal and external auditors in many organizations reviewed for the present report. Segregation of duties and monitoring also rank high in critical findings and recommendations, particularly in audits of field offices as well as operations in emergency and fragile settings. **The Inspectors wish to reiterate that the full and timely implementation by management of the internal control related recommendations by audit bodies is a critical and indispensable element to on effective anti-fraud programme.**

125. A number of programme managers interviewed while acknowledging the impact of fraud on their programmes, expressed concern about introducing what they perceive as "heavy" application of controls on their activities. They see any additional controls as exacerbating the on-going conflict between their main objective of delivering their programmes and the impediment of heavy controls and accountability measures required by donors and legislative/governing bodies. However, as indicated throughout the present report, applying controls in tackling fraud does not necessarily require the introduction of entirely new structures and complex processes that may have serious financial and operational implications. On the contrary, the focus and effort should be in making the existing ones more effective and applying proportionality to address fraud controls based on risk. As discussed, preventive measures and proactively managing fraud is far less costly compared to the costs of having to deal with fraud that has been already perpetrated.

126. The sections below present a number of selected internal control measures that are directly related to the management of fraud risks. An exhaustive list could not be presented given the scope limitations of this review.

A. Accountability frameworks

127. Accountability is defined by the General Assembly as "the obligation of the Secretariat and its staff members to be answerable for all decisions made and actions taken by them and to be responsible for honouring their commitments, without qualification or exception".[55] Within United Nations organizations entrusted with Member State contributions, this concerns in particular the stewardship of those funds, including the prevention of losses due to fraud. Accountability frameworks in United Nations organizations, when properly established, provide the foundation for effective management of fraud risks. By defining the overall organizational accountability environment, such frameworks set the internal and external parameters under which controls operate, inclusive of fraud controls. A number of organizations reviewed have adopted formal accountability frameworks; others have various systems in place without an overarching formal framework.

[55] General Assembly resolution 64/259.

128. To enable organizations to harmonize their respective accountability efforts, the CEB of the United Nations system adopted in 2014 a "Reference Risk Management, Oversight and Accountability Model for the United Nations System."[56] The CEB model relies on the "three lines of defence"[57] approach set forth by IIA. The "three lines of defence" model is often used to communicate the roles played by management, business-enabling functions, and the various independent functions in providing assurance on internal controls. The first line of defence is operations management and employees. The second line of defence is centralized business-enabling functions with specialized skills, such as budget management, risk management, legal and regulatory compliance, and quality assurance. The third line of defence is independent assurance, including internal audit. The three lines are co-dependent, with the need for clear communication between each function, so as to ensure the overall effectiveness of the governance, risk management, monitoring and control practices.[58]

129. Almost half of United Nations system organizations reviewed by the JIU[59] indicated that they have adopted the "three lines of defence" model as a reference for their overall risk management, oversight and accountability framework. For example, the accountability framework that WIPO adopted in 2014 makes specific reference to the model in order to articulate better the roles and responsibilities relating to risk management and internal controls.[60]

130. While existing accountability frameworks do underline in general accountability levels and organizational roles and responsibilities, what is lacking in most United Nations system frameworks, are specific designations of responsibility for addressing fraud, in particular with regard to putting in place appropriate fraud controls. Assessing, "right-sizing" and implementing the relative strength of each line of defence, including putting adequate fraud controls in place, is a joint responsibility of organizations and governing bodies alike.[61]

B. Internal controls

131. Internal controls and control activities comprise all processes designed to provide "*reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance*"[62] As such, anti-fraud controls are an integral part of internal controls and control activities. As overarching policy documents,

[56] CEB Finance and Budget Network, Conclusions from the Working Group on the proposal of a reference risk management, oversight and accountability model for common positioning by the UN system with governing bodies, document CEB/2014/HLCM/FB/3/Rev.1.

[57] IIA, *The Three Lines of Defence in Effective Risk Management and Control* (2013). The model was first suggested by the Federation of European Risk Management Associations and the European Confederation of Institutes of Internal Auditing in December 2011.

[58] CEB/2014/HLCM/FB/3/Rev.1, pp. 17-18.

[59] *State of Internal Audit Function in the United Nations System* (forthcoming, 2016).

[60] WIPO, WIPO accountability framework, document WO/PBC/22/12, p. 4.

[61] CEB/2014/HLCM/FB/3/Rev.1, pp. 17 ff.

[62] See COSO, *Internal Control — Integrated Framework*, p. 3, and International Organization of Supreme Audit Institutions, *Guidelines for Internal Control Standards for the Public Sector* (2013).

internal control frameworks set out guidance for operationalizing and assigning responsibility for internal controls, including fraud controls.

132. Internal and external audit bodies of United Nations system organizations have repeatedly underscored that the complex and risk-prone environment in which United Nations organizations operate demand robust internal control frameworks and a strong focus on fraud among control activities implemented.[63] As discussed in chapter V, rigorous internal control frameworks and standard operating procedures to control fraud and other risks have to be balanced with the need for flexibility and innovation, in particular in fragile and emergency settings. As such, the level of fraud controls in place should vary depending on the specific risk-tolerance level of the organization.

133. In the JIU fraud survey, senior managers of some United Nations system organizations indicated that strong internal control frameworks were the most likely reason for low levels of reported fraud in their organizations. However, this review could not obtain evidence that internal control frameworks that organizations have in place are robust enough to provide assurance on controls that address fraud risks. The various internal and external audit reports mentioned above indicate otherwise.

134. There are 14 United Nations system organizations that have a formal internal control framework in place.[64] A number of these (UNFPA, UNAIDS,[65] WHO and UPU[66]) are either already adhering to, or currently updating internal control frameworks to bring them in line with the COSO framework. Other organizations, in particular specialized agencies, had no comprehensive internal control framework at the time of this review. For example, FAO only recently adopted an internal control framework, which has yet to be fully implemented. While the lack of a formal internal control framework does not necessarily mean no fraud controls are in place, the potential for control failures is heightened, which is a key concern especially in high-risk areas prone to fraud.

135. Furthermore the present review indicates that internal controls in place vary widely, depending on the specific business model and risk areas identified by the organizations. Whether or not internal control frameworks make explicit reference to fraud controls depends on whether organizations perceive there to be particular fraud risks, as established by fraud risk assessments. For example, upon establishing an organization-wide risk register, the United Nations Secretariat did not consider fraud risks to be among the "high level" or "critical" risks for the organization. In UNICEF, however, fraud and misuse of resources is one of the top ERM institutional risk categories.

---

[63] Financial report and audited financial statements for the biennium ended 31 December 2014 and report of the Board of Auditors, A/70/5 (Vol. I) and Corr.1, para. 106; activities of the Independent Audit Advisory Committee for the period from 1 August 2014 to 31 July 2015 (A/70/284), para. 89; OIOS, Audit of the delegation of authority framework in the OHCHR, report 2014/092, para. 10.

[64] The 14 organizations that have a full internal control framework in place are: IAEA, ICAO, UNDP, UNESCO, UNFPA, UNHCR, UNICEF, UNIDO, UNOPS, UN-WOMEN, UPU, WFP, WHO and WIPO.

[65] UNAIDS noted that it is in the development stage of the internal control framework in line with COSO 2013.

[66] UPU noted that it is already applying the COSO framework, since it evaluates principle 8 ("assesses fraud risk") on a yearly basis.

136. In most United Nations system organizations fraud is not being considered a high-level corporate risk. As such, there is a tendency of senior managers and staff not to be sufficiently compelled, through the frameworks and arrangements that govern internal control mechanisms, to act and strengthen fraud-related controls and control activities in place.

137. The implementation of the following recommendation is expected to enhance the mitigation of fraud risks through improved effectiveness and adequacy of the organizations' internal control frameworks.

Recommendation 7

The executive heads of the United Nations system organizations, if they have not already done so, should initiate a review of their internal control framework to ensure that proportionate anti-fraud controls do exist and that fraud risks identified in the fraud risk assessments are adequately addressed in the internal control frameworks.

138. *Statements of internal controls.* It is good practice to require managers to underwrite written attestations of proper controls in their respective functional areas of work.[67] On an aggregate level, such attestation mechanisms can then serve in the preparation of annual statements on internal controls, which are in essence a letter signed by an organization's senior executive outlining their approach to, and undersigning their responsibility for, internal controls. That statement forms part of the financial statement of an organization and should include an assertion of the state of affairs with regard to internal controls, risk management and governance processes, as well as of the adequacy of fraud controls in place.

139. Such written attestations required from managers are "a very powerful tool to push accountability down the management line".[68] A few organizations, such as ICAO, ITU, UNESCO, WFP WHO, WIPO and WMO already prepare an annual statement on internal controls and the United Nations Secretariat plans to introduce one by 2018.[69] When such statements are audited by internal audit offices, they provide even higher assurance of an organization's internal control framework. This is the case, for example, at WFP, which has been at the forefront of developing such statements after having first implemented one in 2011. The WFP internal audit office has audited the internal control assurance process in 2014 with overall good results.[70] This reflects a good practice that can be followed by other organizations once a process for the attestation of a statement on internal controls has matured.

140. The implementation of the following recommendation is expected to enhance accountability and contribute to the effectiveness of the organization's anti-fraud programme through instituting Statements of Internal Controls in line with good practices.

[67] Accountability frameworks in the United Nations system (JIU/REP/2011/5), benchmark 12.
[68] Accountability frameworks in the United Nations System (JIU/REP/2011/5), para. 111.
[69] See A/70/284.
[70] WFP, Office of the Inspector General, Internal audit of WFP's Internal Control Assurance Process 2013, document AR/14/14.

Recommendation 8

When introducing or updating statements of internal controls, the executive heads of the United Nations system organizations should ensure that the statements address the adequacy of organization-wide anti-fraud controls, in accordance with good practices and applicable international standards. In the absence of a formal statement of internal controls, executive heads should certify in their annual reports to legislative and governing bodies that their organization has in place proportionate anti-fraud controls based on fraud risk assessments, and that appropriate fraud prevention, detection, response and data collection procedures and processes exist.

141. Areas of control activities with particular relevance to fraud risk mitigation include, inter-alia, the following: (a) segregation of duties; (b) a clear delegation of authority, including for payment approvals, authorization, verification, certification, reconciliation and review of operating performance; (c) the safeguarding of assets; and (d) fraud controls in procurement and contract management.

142. *Segregation of duties* is a key internal control intended to minimize the occurrence of errors and/or fraud. Segregating duties among personnel ensures that no employee has the ability to both perpetrate and conceal fraud in the normal course of his/her duties. Segregation is required for duties related to the authorization or approval duties from the custody of assets and the recording/reconciliation and control of financial transactions. While a number of United Nations organizations, such as IAEA, UNFPA, UNIDO, UNESCO, WFP and WIPO have segregation of duties arrangements integrated in their ERP systems, challenges remain when it comes to small field offices with few staff, or in emergency contexts, that do not allow for proper segregations. Centralizing duties, especially in procurement cases, or at least subjecting existing cases to additional monitoring, such as done by UNICEF supply division, is a good practice to mitigate associated fraud risks. **Automated controls on the basis of ERP systems that delegate, for example, the authority for review and approval to central units when the proper field segregation of duties is not feasible, can help to mitigate the risk of fraud and should be incorporated and implemented wherever necessary.**

143. *Delegation of authority* is another key fraud prevention and detection element that ensures that roles are clearly defined and responsibilities apportioned. For example, at WFP, purchase orders and requisitions cannot be modified without resetting previous releases, which prevents unauthorized and potentially fraudulent activities. Appropriate delegation of authority is a functional necessity in the complex and dispersed United Nations activities worldwide. Against this background, BOA recommended in a recent report that organizations should have a central repository of all delegations of authority.[71] In 2004, JIU had reviewed delegation of authority arrangements within the United Nations system and presented eight principal benchmarks for effective delegation arrangements. It is

[71] A/70/322, paras. 81 ff.

recommended that organizations continue to apply these benchmarks when reviewing and reforming delegation of authority procedures.[72]

144. *Safeguards to ensure organizational assets are protected* from fraudulent activities are another area of importance as fraud related asset losses is a frequent occurrence in the United Nations system. Such safeguards should cover the full cycle of asset acquisition, recording, disposal and write-off. Regular asset inventories and certification processes ensure their proper custody. For example, UNFPA has specific policies and procedures for fixed asset management and, increasingly, organizations such as WIPO use the functionality of their ERP systems for the management of assets.

145. *Robust fraud controls in procurement and contract management*[73] are particularly needed because these areas are highly susceptible to fraudulent activities such as collusion between vendors or between vendors and staff, bribes, bid rigging, kickback schemes, splitting of contracts to remain below the prescribed threshold of delegation of authority, undue influencing of contract selection, as well as change order and invoice abuse, such as double billing schemes. In particular, organizations with large-scale field operations, such as UNDP, UNFPA and UNICEF, but also others such as FAO and UNESCO, indicated in their response to the JIU questionnaire that procurement fraud is one of the top two categories in terms of frequency of cases and high volumes of associated losses.

146. Reported shortcomings of fraud controls in the case of "big ticket" procurement actions, are often related to circumventing established procedures and processes. For example, a recent audit report by OIOS on recommendations on procurement activities, as well as reports by the BOA and the JIU, have identified frequent violations of authority levels and compliance with established procedures and processes (competition requirements, bid opening etc.).[74]

147. Another high risk area is local and decentralized procurement especially in countries that rank high in the World Bank corruption index, where the operating environment may be conducive to corruption, nepotism and collusive practices. Often, organizations are compelled to operate in unfamiliar markets and with a limited number of suitable vendors and suppliers which creates potentially an environment for collusion or bid ringing. Another factor is that procurement under a certain threshold is often not reviewed by any procurement committee. There are also internal shortcomings, such as limited capacity in reviewing bids, improper segregation of duties and lack of other checks and balances. The above constraints significantly impede transparent and competitive procurement processes and substantially increase fraud risks. Many interviewees, in particular those with extensive operational experience in these environments, see these constrains as a main cause for large amounts of fraud losses in the United Nations system. Similarly, several respondents to the JIU fraud survey have flagged procurement-related fraud as a recurrent and serious issue.

---

[72] Delegation of authority and accountability, part II of the Series on Managing for Results in the United Nations System (JIU/REP/2004/7), paras. 6-38.

[73] Also refer to related sections on vendor due diligence (chap. VII, sect. E) and vendor sanction regimes (chap. X, sect. C).

[74] OIOS, Review of issues identified in recent oversight reports on procurement activities (AH2012/513/02).

148. Regarding fraud controls during post-award contract management, a recent JIU report[75] found a lack of sufficient monitoring and inadequate mitigation of risks associated with the management of vendor contracts throughout the United Nations system. The report concluded that post-award contract management represented one of the highest risk areas in the procurement life cycle. Recurrent challenges mentioned in the report were insufficient vetting of past performance of unqualified vendors, inadequate contract performance monitoring, unauthorized change orders, failure to manage contracts within their expiration dates and undocumented contract extensions.

149. A number of organizations reviewed have been taking measures to mitigate fraud risks along the full procurement and contract management cycle. Such measures include fraud controls enumerated in sound policies such as "no gifts, no hospitality" for procurement staff, vendors required to disclose previous debarments and so on. In this regard, many organizations have in recent years established contract review and/or procurement review committees, e.g. in UNOPS, FAO, UNFPA, UN-Women and UNDP, in order to ensure compliance with established due diligence and due process regulations against procurement/contract management fraud. Because of the risk-prone nature of their work, it is the practice in some organizations for staff involved in procurement and contract management to receive regular and targeted anti-fraud training (see chap. IV, sect. C above). Procurement handbooks in some organizations reflect roles and responsibilities with regard to fraud, such as the responsibility of authorized procurement officials to conduct due diligence of vendors during identification and sourcing. For example, in IMO, a new vendor can only be added to the vendor register after due diligence has been performed by various organizational entities, such as by the procurement officer to ensure the suitability and reliability of the vendor, by the finance department to verify good financial standing and by technical experts to confirm standards of services and goods.

150. **The Inspectors reiterate the importance of compliance with the recommendations made in the JIU procurement and contract management-related reports (JIU/REP/2014/9, JIU/REP/2013/1 and JIU/NOTE/2011/1) and in addition suggest that local procurement authorization thresholds should be determined on the basis of respective risks, taking into account, inter alia, the size of the office and the risk environment it operates in, procurement volumes, existing procurement capacities, the level of certification of staff, adequate segregation of duties and the delegation of authority arrangements.**

C. Codes of conduct

151. A written code of conduct is one of the most important vehicles to communicate to staff key standards of acceptable and prohibited behaviour, including fraud and other misconduct. Codes of conduct advance fraud awareness, as they bring together standards for ethical behaviour that may be defined elsewhere, including in organization's financial rules and regulations, human resource handbooks, procurement manuals etc. According to an ACFE survey of

[75] Contract management and administration in the United Nations system (JIU/REP/2014/9).

1,483 actual fraud cases in the private and public sector around the world,[76] a strong code of conduct helped to reduce the median fraud losses by 46 per cent and the duration of how long a fraud scheme lasted before being discovered by 37 per cent on average.

152. Provisions governing the ethical conduct of staff in United Nations system organizations are normally contained in a number of sources, including the Charter of the United Nations and the United Nations staff rules and regulations. The standards of conduct for the International Civil Service, adopted by the International Civil Service Commission (ICSC),[77] constitute the central reference point for regulations on staff conduct and ethical values within the United Nations system based on the belief that, while organizations' internal cultures vary, they face similar ethical challenges. The latest ICSC version of the standards was approved by the General Assembly in 2013.[78] In their current form, the standards are particularly focused on the independence and impartiality of international civil servants, but do not specifically mention fraud or focus on the provision of practical guidance to assist staff in making ethical choices. Thus, an opportunity is missed to raise fraud awareness and to provide guidance to staff on appropriate standards of behaviour, as well as to direct them to the available mechanism for reporting.

153. The majority of organizations within the United Nations system make reference to the ICSC standards of conduct. However, two organizations have chosen not to adopt the standards (UNOPS and UNHCR)[79] and have developed their own codes of conduct to suit their particular organizational needs.[80] ICAO, on the other hand, has adopted a version of the ICSC standards that has been adapted slightly to match its particular circumstances. BOA has issued a specific recommendation to the United Nations Secretariat to adopt a clear code of conduct to raise fraud awareness.[81] An earlier initiative for a system-wide code of ethics for United Nations personnel developed by the Ethics Panel of the United Nations was deferred by the General Assembly and, after much debate, the code was eventually incorporated into the 2013 revision of the ICSC standards.[82]

154. While the existing codes of conduct, including the ICSC standards, are addressed mostly to staff members (including managers), a good practice is to extend the code of conduct to non-staff and third parties. Such practice is partially followed by UNIDO in its Code of Ethical Conduct that is also applicable to "holders of (special) service agreements, individuals on reimbursable and non-reimbursable loan, Goodwill Ambassadors, and other individuals associated

[76] ACFE, *Report to the Nations on Occupational Fraud and Abuse: 2010 Global Fraud Study* (Austin, Texas, 2010).

[77] The standards were originally introduced in 1954 by the International Civil Service Advisory Board, which subsequently became ICSC.

[78] General Assembly resolution 67/257.

[79] Report of the International Civil Service Commission for 2009 (A/64/30).

[80] Report of the International Civil Service Commission for 2009 (A/64/30), para. 22.

[81] Financial report and audited financial statements for the biennium ended 31 December 2013 and report of the Board of Auditors, A/69/5 (Vol. I), para. 136.

[82] The General Assembly initially requested the development of a system-wide code of ethics in its paragraph 161 (d) of its resolution 60/1.

with UNIDO".[83] Also, UNESCO, as per its Human Resources Manual and respective contract provisions, formally extends the standards of conduct to temporary personnel such as service contractors.

155. It should also be noted that that the United Nations Global Marketplace (UNGM), through which the majority of United Nations system procurement is transacted, has established the United Nations Supplier Code of Conduct. The Code covers labour and human rights, environment and ethical standards, and calls upon vendors to adhere to highest ethical standards, respect local laws and not to engage in corrupt practices, including fraud (para. 18). However, the language used on the UNGM platform is relatively weak in that it only places an "expectation" on vendors, instead of, for example, framing adherence to the provisions contained in the Code as a requirement.

156. In order to enforce compliance of staff and senior management with codes of conduct, organizations frequently instigate the good practice of an affirmation process. In such a process, as recently established at ILO,[84] a person confirms that he or she has read, understood and will comply with a code of conduct. This facilitates and makes more effective any potential legal action against non-compliant staff and is considered a cost-effective practice for fraud prevention. Paper-based or electronic affirmation processes usually take place upon entry of new staff within an organization, but could also be re-confirmed in regular intervals or upon any revisions of the code of conduct. Some organizations, such as ILO and UNDP, have also established additional affirmation processes for staff in high-risk positions, such as in procurement. Lastly, for third parties such as implementing partners, it is good practice for an affirmation process to be part of the standard legal agreements (see section F below).

157. **It is recommended that the executive heads of United Nations system organizations, in order to raise awareness of the applicable standards of conduct, adopt a written affirmation process for all new and existing staff, whereby staff and managers confirm their knowledge, understanding and continued compliance with the standards of conduct of ICSC.**

D. Financial disclosure and declaration of interest programmes

158. Most United Nations organizations reviewed have a financial disclosure and/or declaration of interest programme in place. This is a significant improvement since earlier years and a positive development.[85] The main focus of these programs is on declaring and mitigating potential and actual conflicts of interest[86] arising from

[83] UNIDO, Code of Ethical Conduct, Director-General's bulletin UNIDO/DGB/(M.).115; footnote 1 of the Code, extends the term "personnel" further to "including, but not limited to interns and other parties in contractual relations with UNIDO as contained in the provisions of this Code".

[84] See ILO, Ethics and Standards of Conduct, circular DIR 01/2015, and Ethics in the Office, office directive IGDS No. 76 (Version 1).

[85] In 2010, CEB had conducted a survey which found that only 11 out of 16 organizations had a financial disclosure programme in place (see minutes of the CEB-Finance and Budget Network, document CEB/2010/HLCM/FB/30).

[86] See the report of the Secretary-General on personal conflict of interest (A/66/98).

either financial holding or outside activities and thus they are seen as contributing to fraud and corruption prevention and detection.

159. In terms of coverage, existing programmes are primarily focused on senior managers as well as selected staff in risk-prone functions, in particular procurement, financial transactions, contract management, oversight functions (ethics, audit, audit committees etc.) and certain elected officials.[87] Of the organizations that provided information to JIU, only the programmes of the World Tourism Organization (UNWTO) and WHO are limited to senior management without additional coverage for functional staff in high-risk areas. **As officers managing implementing partners are similarly prone to fraud-risks, it is recommended that organizations review the extent to which they need to be included in the financial disclosure programme, as appropriate.**

160. Where a potential conflict of interest is revealed through a financial disclosure programme, staff would normally be advised to divest themselves of financial holdings or to recuse themselves from a particular activity or aspect of their official functions. This is the case, for example, under the programme of the United Nations Secretariat, which applies to several entities, including UNHCR, UNRWA and OHCHR.[88] At UNDP and UNICEF, a good practice is to issue guidance letters to concerned staff on how to prevent potential conflicts of interest from materializing. The letters need to be countersigned by staff in order to confirm that they have understood the guidance. A number of organizations conduct training programmes and provide substantial assistance for current and potential participants in their financial disclosure programmes, in order to enhance compliance and to reduce erroneous declarations. For example, the United Nations Secretariat uses online conferencing services to provide real-time assistance to filers.[89]

161. The information obtained through financial disclosure programmes is normally not publicly disclosed. However, the United Nations Secretariat has in place the good practice of senior public officials (at the level of Assistant Secretary-General, Under-Secretary-General and above) making public their financial disclosure statements on a voluntary basis.

162. In terms of verification of information provided under financial disclosure programmes, in the majority of programmes it is typically based on an honour system complemented by further verifications processes, including by third parties, for a subset of reports that were selected randomly. A targeted, risk-based approach to verification of financial disclosure programmes and conflict of interest declarations with attention on high-risk red flags[90] is best practice and should be considered by United Nations system organizations.

163. **It is recommended that United Nations system organizations conduct a review of their financial programmes for disclosure and declaration of interest,**

[87] See the recommendation on the coverage of financial disclosure programmes in JIU report on oversight lacunae in the United Nations system (JIU/REP/2006/2).

[88] See Secretary-General's bulletin (ST/SGB/2006/6).

[89] Report of the Secretary-General on the activities of the Ethics Office (A/70/307).

[90] World Bank and UNODC, *On the Take: Criminalizing Illicit Enrichment to Fight Corruption* (Stolen Asset Recovery Initiative, 2012).

with a view to enhancing their effectiveness, and determine the adequacy of the coverage of staff required to participate in the programme.

E. Anti-fraud due diligence: screening of staff and third parties

164. Anti-fraud due diligence measures comprise various activities aimed at subjecting a person or third party to systematic scrutiny of any indications of past or present fraudulent activity or behaviour prior to engaging in a business relationship with them. Due diligence can be targeted at (a) internal staff and (b) third parties (consultants, vendors, implementing partners etc.). These due diligence measures are based on the understanding that it is cost-effective to take necessary precautions and conduct adequate screening prior to engaging a potentially fraudulent candidate as staff or formalizing a partnership with a third party, so as to avoid challenges afterwards, including lengthy and costly legal processes. Good practice calls for due diligence measures not to stop at the point of engagement, but be extended, on a risk basis, to continued scrutiny and screening, at regular intervals, of existing commercial and employment relationships.

Screening of staff

165. Anti-fraud due diligence measures for United Nations staff can be implemented through various measures, including: self-declarations to disclose potential conflict of interests; self-declarations on prior disciplinary measures; automated verifications of academic credentials (done, for example, by UNFPA) to prevent fraudsters from joining the organization's workforce; checks on former United Nations staff against prior dismissals (done by the United Nations Secretariat)[91] and specific checks for new staff in high-risk posts. A few organizations, such as UNOPS, WIPO and UNFPA, use the services of professional firms to conduct due diligence checks. UNDP screens candidates for senior positions, including for any prior record of human rights violations, and require all newly hired staff to complete a conflict of interest disclosure form. However, previous JIU reports on human resources-related issues found evidence of inadequate reference and other checks at most United Nations organizations and made a number of recommendations to that effect.[92]

[91] In their response to the JIU questionnaire, the Secretariat indicated: "A former staff member of the United Nations Common System is pre-flagged for a manual Human Resources review whether he/she had previously been summarily dismissed or separated for misconduct [...]. If yes, the applicant is not reviewed further."

[92] Staff recruitment in United Nations system organizations: a comparative analysis and benchmarking framework – the recruitment process (JIU/NOTE/2012/2), para. 66 (on reference checks).

166. Box 2 below contains a non-exhaustive list of good practices in this regard.

Box 2. Good practices in human resources-related due diligence measures

There are a number of human resources-related due diligence measures to mitigate potential fraud risks, including:

- *Verification of credentials*: Checks to verify personal information and to confirm work history can help to uncover falsified or embellished credentials
- *Reference checks*: Reference checks can uncover red flags concerning personal integrity and reputational issues, which may be incompatible with employment
- *Background checks*: Background checking for criminal records or the state of affairs of personal finances can be a source of additional information to assess applicants. The nature and extent of background checks in normally governed by law and prospective employees may have to consent
- *Cross-checks on past disciplinary action*: Inquiries with other United Nations organizations, tribunals etc. about past disciplinary action of individuals can complement due diligence measures

Source: JIU compilation of good practices, based on questionnaire responses and literature review.

167. Staff transferring to employment with another United Nations entity is a common occurrence within the United Nations system. However, many interviewees expressed concern with the lack of information-sharing among United Nations organizations regarding past and ongoing disciplinary actions of prospective applicants. While a few organizations, in particular the United Nations Secretariat, stated that they conduct cross-checks on past disciplinary actions within the United Nations common system, such practices are not applied systematically and for all types of contracts, despite offering clear benefits in terms of preventing, inter alia, fraudulent activities.[93] Notwithstanding issues related to confidentiality and due process (e.g. presumption of innocence), appropriate language on the application forms requiring disclosure of the applicant being a subject of past or current investigation or disciplinary action by another United Nations entity, should be considered for adoption by all organizations that do not currently have such a measure in place (see the discussion in chap. X on this issue).

168. Conducting exit interviews and a systematic analysis of resignation letters of staff leaving organizations for reasons of retirement, resignation, termination or otherwise, is a good source of information for human resource managers to establish whether there were or are any integrity issues that need to be taken into account. While this is a good practice in many private sector organizations, it is not a common practice in the United Nations system.

[93] Staff recruitment in United Nations system organizations: a comparative analysis and benchmarking framework — institutional framework (JIU/NOTE/2012/1), p. 12.

Due diligence for vendors[94]

169. In the context of contracting with potential vendors, a number of United Nations system organizations have rights to inspect the books of such vendors and suppliers. However, as reported by interviewees and indicated by external and internal auditors, most organizations rarely do so. At a minimum, such inspections should take place for major contracts and in cases of vendors with multiple contracts, regardless of value.

170. Having robust electronic databanks of registered vendors and sharing them across the United Nations system are important prerequisites for respective due diligence measures (also see chap. X below on vendor sanctioning). The main platform for sharing vendor related information throughout the United Nations system is the Global Market Place (UNGM).[95] It is an automated vendor registration system for procurement that provides a common portal for information on vendors and includes capability for checking vendor performance and previous involvement in United Nations procurement services. One of its aims is to streamline procurement processes so as to reduce time and increase efficiency.

171. Since the launch of UNGM 2.0, 10 agencies have integrated their procurement systems with UNGM, so that when vendors register with UNGM that information is transmitted directly and automatically into individual agencies' procurement systems, which ensures up-to-date information For example, following the deployment of Umoja in peacekeeping operations, more than 75,000 vendor records were cleansed and reduced to approximately 7,000, which were then uploaded onto UNGM and synchronized with Umoja.[96]

172. Previous JIU reports[97] called for the establishment of databases for information-sharing on vendor performance evaluations within organizations and the United Nations system. In interviews for the present report the UNGM administrator indicated UNGM plans to expand into this area as early as in 2016 (see also chap. X, sect. E below).

173. It was also observed that United Nations organizations engaging in the selection of vendors have to guard against the risks emanating from shell companies. Shell companies, which may take the form of a mailbox registered in an offshore tax haven, are often the source of fraudulent activities, especially in fragile and conflict-prone environments, and they played a crucial role in the "oil-for-food programme" fraud scheme. For external verification of companies to be engaged as vendors or contractors, some organizations reviewed use commercial firms such as Dun & Bradstreet or Kompass to provide company and credit information verification services.

[94] Refer also to related sections on controls in procurement and contract management (chap. VII, sect. B) and vendor sanction regimes (chap. X, sect. C).

[95] See www.ungm.org; see also, on the status of UNGM, CEB/2015/HLCM_PN/17, para. 52.

[96] Report of the Secretary-General on the fourth progress report on the accountability system in the United Nations Secretariat (A/69/676).

[97] Contract management and administration in the United Nations system (JIU/REP/2014/9), recommendation 8, and Corporate consultancies in United Nations system organizations: overview of the use of corporate consultancy and procurement and contract management issues (JIU/NOTE/2008/4), recommendation 18.

Due diligence for implementing partners

174. Many United Nations organizations rely on implementing partners to deliver large parts of their operations. Implementing partners can be national and international NGOs, national governmental entities, local civil society actors and others. A previous JIU report[98] found several weaknesses with regard to due diligence measures for implementing partners before, during, and after entering into business relations with them. **The evidence base established in that report and the respective recommendations are deemed highly relevant for the United Nations system response to the rising challenge of fraud related to implementing partners.** Furthermore, implementing partner fraud was ranked high by respondents of the JIU fraud survey among a list of seven common fraud types, with one quarter of respondents expecting a case of implementing partner fraud to occur within the next 12-24 months.

175. The capacity assessments[99] ("macro" and "micro assessments") under the harmonized approach to cash transfers (HACT)[100] are designed to standardize due diligence activities further. UNDG approved a revised HACT framework in 2014 and it is being fully applied by UNDP, UNICEF and UNFPA as the sole risk management framework for working with implementing partners.

176. However, it should be noted that HACT does not specifically put emphasis on or address in detail fraud specific risks of implementing partners. Implementing partners are a diverse group of entities with various legal setups (NGOs, civil society, government entities, etc.). In the case of NGOs, basic organizational information, such as creditor data, legal status etc., is often lacking or not readily available.[101] While HACT covers their compliance and alignment with the governance arrangements of the United Nations system, as well as with administrative, technical and financial capacities, gaps remain, such as with regard to systematic reference checks on the senior management of the NGOs and their key personnel (procurement, finance etc.)[102] as well as the lack of an affirmation process for all staff to adherence to organization's standards of conduct. In the case of

[98] Review of the management of implementing partners in United Nations system organizations (JIU/REP/2013/4). See also Oversight lacunae in the United Nations system (JIU/REP/2006/2); Ethics in the United Nations system (JIU/REP/2010/3); Accountability frameworks in the United Nations system (JIU/REP/2011/5).

[99] The purpose of a macro-assessment is to ensure adequate awareness of the public financial management environment within which agencies provide cash transfers to IPs. Micro-assessments, on the other hand, assess the IP's financial management capacity (i.e., accounting, procurement, reporting, internal controls, etc.) to determine the overall risk rating and assurance activities.

[100] The *Harmonized Approach to Cash Transfer* (HACT) framework was first introduced in 2005 and substantially revised in 2014 to take into account deficiencies raised by the UNDG HACT Advisory Committee, and by the *Joint Audit of the Governance Arrangement for the Harmonized Approach to Cash Transfer (HACT)* (2012). Under HACT, United Nations system organizations select methods for transferring cash on the basis of risk assessments of the IPs that determine the required level of monitoring and auditing for the work. The level of assurance for cash transfers moves from project level controls and audits, to assurance derived from system-based assessments and selective audits.

[101] Ibid.

[102] See "Micro Assessment questionnaire", question No. 3.9, in UNDG, *HACT framework* (2014) and others.

follow up when implementing partners are government entities the HACT instructions and guidance remain silent.

177. Other entities such as UNHCR and OCHA use similar, if not expanded, versions of the HACT due diligence processes when dealing with third parties. The UNHCR manual for implementing partners and related checklists for work plans contain many of provisions for systematic reference checks of NGO staff and senior management and represent good practice in that regard.

178. In addition to the issues mentioned above, other key risk factors that organizations need to guard against when dealing with implementing partners are risks similar to those of dealing with vendors and suppliers: overstatement of costs, overstatement of quantity of product or services delivered deviations from quality specifications, delays in delivery of products or services, and non-delivery.[103] One particularity of the required due diligence process concerns the need to guard against the possibility of double contracting or billing by some implementing partners to multiple partners or donors for the same activities or programmes.[104]

179. Due diligence processes need to verify, via strengthened monitoring and regular auditing and inspections, that adequate capacities exist to deliver the relevant products or services and systems are in place and functioning to safeguard against misappropriations of funds. For example, the revised HACT framework now includes provisions for joint assurances in cases of implementing partners shared between two or more United Nations entities. A differentiated approach is viewed as most efficient and effective in this regard, focusing verifications and inspections on high-risk and/or high-value projects.

180. That the selection and management of implementing partners is a high risk area for potential fraud, is also demonstrated by a number of reported high value fraud cases. For instance, the investigation division of OIOS of the United Nations Secretariat in 2014 and 2015 reported cases in Somalia showing that more than 6.7 million US$ were lost through fraud committed by implementing partners. This represents more than 73 per cent of the United Nations funds disbursed to be fraudulently claimed or unsupported during that period.[105] This is in addition to investigation cases of previous years, and in view of the fact that several related investigations were still ongoing at the time of the preparation of the present report.

181. **The Inspectors reiterate the importance of full and timely implementation of the pertinent recommendations of the aforementioned JIU report on implementing partners (JIU/REP/2013/4),[106] in particular that the selection and management of implementing partners is based on i) in-depth assessments of their capacities and due diligence, ii) sound legal agreements to safeguard United Nations interests and funds, iii) risk-based monitoring and reporting,**

[103] These factors of potential fraud are selection, price, quality, quantity and delivery.

[104] Review of the management of implementing partners in United Nations system organizations (JIU/REP/2013/4), p. 43.

[105] A/70/318, paras 65-68; A/69/308, paras 44-48.

[106] Review of the management of implementing partners in United Nations system organizations (JIU/REP/2013/4), p. 43. See also A/RES/69/249, op. 20. The BOA has also addressed the issues related to implementing partners in several of its recent reports, and also provided an update on the state of affair and implementation of its recommendations for selected organizations (see e.g. A/70/322, paras 35-41, A/69/5 (Vol. I), paras. 90-128, and A/70/5/Add.6, pages 48, 49, and 60).

iv) robust auditing and evaluation, and v) improved fraud awareness, training and guidance to support a systemic anti-fraud effort when engaging and managing implementing partners. Also, more needs to be done to assure investigation rights over third parties and to improve sharing of information on implementing partners among organizations at the country, regional and headquarter levels (see i.e. chapter IX, section B, chapter X, section E and chap. XI, sect. D of the present report).

F. Updating legal instruments for third parties

Anti-fraud clauses for vendors and implementing partners

182. As discussed in previous chapters, anti-fraud policies in most United Nations system organizations have historically applied only to staff members, consultants and interns. Anti-fraud policies were silent on the presence of vendors and implementing partners who, in many organizations, are the main vehicles in the delivery of programs.

183. In recent years most United Nations system audit and oversight charters have been updated to extend the mandate of the oversight services to include the right to audit and the right to investigate third parties including implementing partners. Furthermore, JIU report (JIU/REP/2013/4)[107] has recommended that the agreements and memorandums of understanding with implementing partners should contain provisions and clauses to the same effect. A review of a sample of agreements, conducted for the present report, showed that most organizations, in particular those that have recently updated their anti-fraud polices and/or their implementing partner policy, such as FAO, UNFPA, WFP, UNHCR and the Office for the Coordination of Humanitarian Affairs (OCHA), have aspects of such provisions in place. Notably, UNDG has, in mid-2015, also updated its legal agreements that govern multi-donor trust funds and other joint activities. However, the provisions in a number of organizations vary in terms of comprehensiveness, detail and robustness. Some agreements only allow for audits or inspection rights but not investigations. Some extend the oversight rights to the subcontractors of the implementing partner, but others do not. Finally, some organizations have not included any relevant provisions at all in the agreements or memorandums of understanding.

184. A non-exhaustive list of fraud-related provisions for agreements with third parties is shown in box 3 below.

Box 3: Fraud-related provisions for legal agreements with third parties

- DEFINITIONS OF FRAUD AND OTHER KEY TERMS (MISCONDUCT, FINANCIAL WRONGDOING, MISAPPROPRIATION ETC.)
- OBLIGATION TO REPORT ANY SUSPECTED FRAUD IMMEDIATELY (INCLUDING REFERENCE TO THE UNITED NATIONS ORGANIZATION'S FRAUD HOTLINE/WEBSITE)

[107] Review of the management of implementing partners in United Nations system organizations (JIU/REP/2013/4), p. 43.

- MINIMUM STANDARDS AS TO INTERNAL CONTROL AND ACCOUNTABILITY STANDARDS, INCLUDING FOR FINANCIAL MANAGEMENT, PROCUREMENT, ENGAGING OF SUBCONTRACTORS ETC.
- SPECIFIC TERMINATION CLAUSES IN CASES OF FRAUD, AND CLAUSES TO WITHHOLD PAYMENTS IN CASES OF CREDIBLE ALLEGATIONS OF FRAUD
- ARBITRATION CLAUSES
- WHISTLE-BLOWER PROTECTION CLAUSES (INCLUDING REFERENCE TO UNITED NATIONS ORGANIZATION'S FRAUD HOTLINE/WEBSITE)
- REQUIREMENTS TO PROVIDE INFORMATION, ACCESS TO DOCUMENTS/SITES/OPERATIONS/STAFF, AUDIT, INSPECTION AND INVESTIGATION RIGHTS, AND DUTY TO COOPERATE WITH AUDITS, INVESTIGATION AND INSPECTIONS, INCLUDING FOR SUBCONTRACTORS
- SANCTIONS AND REIMBURSEMENT OF DAMAGES
- REFERRALS TO NATIONAL LAW ENFORCEMENT AUTHORITIES

Source: JIU 2015.

185. The need for protecting the organization against fraud committed by third parties was also supported by the view of staff at large in the JIU fraud survey. When asked about the protection against fraud emanating from different parties, respondents indicated the least confidence in the adequacy of protection against fraud involving implementing partners and vendors. Only 27 per cent of respondents were fully confident that protection was adequate. Similar concerns were voiced during interviews with staff in the field that interfaces with third parties more frequently.

186. To guarantee and safeguard the interests of the United Nations system, concomitant control and mitigation measures are necessary, which include, as discussed above, robust legal instruments, i.e. implementing partner agreements and memorandums of understanding. The right to appropriate oversight on the funds transferred, including investigation, audit and inspection of the implementing partners and subcontractors, is only one of the indispensable elements of such agreements; other provisions include an obligation to report fraud, adequate internal control framework, recovery of assets, arbitration etc.

187. The reader is also referred, in this context, to related recommendations on chapter X below on the sanction and disciplinary regime of organizations, as well as the process for referrals of cases to national authorities for criminal and civil proceedings, including asset recovery.

188. The implementation of the following recommendation is expected to enhance the effectiveness and efficiency of the organization's anti-fraud programme.

Recommendation 9

The executive heads of the United Nations system organizations should instruct their legal offices to review and update the legal instruments for engaging third parties, such as vendors and implementing partners, with particular attention to anti-fraud clauses and provisions.

G. Automation of fraud controls

189. Information technology-based systems, such as ERPs, that automate internal controls and monitoring provide a boost to anti-fraud activities and are a crucial part of an organization's fraud risk management programme. The biggest benefit of automated controls is that they offer basic checks in real time, in particular for standard and routine business operations. These include the processing of payments, the approval of travel, due diligence checks related to procurement, recruitment processes etc.

190. Automation offers, inter alia, intelligence and analytics capability, real-time data, monitoring of business operation metrics, dashboards and other measures aimed to provide information and generate fraud-related knowledge. For example, the tracking of all reports of fraud and case outcomes can greatly enhance fraud risk management by providing tangible information to compare against industry benchmarks, assist the analysis of trends and help guide the fraud response.

191. Automated anti-fraud controls and monitoring are especially effective in detecting fraud. Rules-based filters help to identify potentially fraudulent transactions and behaviour, data analysis supports the detection of anomalies and abnormal patterns, predictive models identify potential fraud risks, and social networks analysis helps to detect cases by systematically analysing links between people and transactions.

192. A number of organizations, notably WFP, ITU, UNESCO and IAEA use specialized software tools, such as IDEA, agileSI and ACL, to interrogate existing data for suspicious activity, red flags, duplicate payments etc. that may indicate potential fraud. Other proprietary software solutions used by the United Nations system include Active Data for Excel and SAS. These programmes are mainly used by oversight offices and auditors. It should be noted that defrauding patterns change and evolve continuously in line with developments in organizations and, as such, there is a need to adapt information technology detection systems, especially if they have already been in use for significant periods.

193. While this review did not look in detail at the functionality of ERPs and other automation systems in the United Nations system, it was observed that most organizations have basic forms of automated controls integrated in their ERP systems. The typical ERP system in the organizations reviewed has functionality that provides for an audit trail, user authorization and assignment of different roles on the basis of segregation of duties; some thresholds established for high-value transactions that trigger additional review processes, supervisor approvals, and dashboards and automated report generation for performance and compliance

indicators. These are functionalities that support fraud prevention and detection. However, interviewees indicated there is much room for improvement in this area as the anti-fraud capabilities of ERP systems have not been fully explored.

194. For example, ERP systems need to provide proper safeguards against management overrides of existing controls. Management overrides — interventions aiming to circumvent existing internal controls based on privileged access and/or authority — are a frequent factor in fraudulent activity, in particular in combination with staff involved in collusion. Such overrides could involve, inter alia, requests for disbursement without proper supporting documents, changes to orders, purchases or hires without appropriate authorizations etc. Management overrides are often prevalent in high-profile fraud cases with substantial losses. An ERP system can log any overrides of existing controls by management or staff, thereby establishing patterns and corroborated evidence of potential fraud. **Information shared during interviews and evidence collected suggest that management overrides are an area of concern that needs to be addressed with urgency across the United Nations system by, inter alia, limiting the application of overrides, documenting their occurrence and checking their results.**

195. The implementation of a new or the update of an existing ERP offers an opportunity to organizations to significantly enhance their efforts to strengthen fraud detection and prevention by integrating strong controls and cutting-edge functionality in their automation systems. Such may be the case at UNRWA and UNOPS, and most notably the United Nations Secretariat and its subsidiary organs with their Umoja system. However, while the Umoja team has a business intelligence unit that may look at aspects such as automated fraud controls, there was no indication, at the time of the present report, that specific and dedicated anti-fraud functionalities had been incorporated or planned in this system.

196. One good example of fraud controls automation was observed at UNHCR, which during the 2015 upgrade of its ERP system used the opportunity to design and prepare for implementation an automated software package for strengthened automated controls attached to its ERP system, which could run queries for anomalies and unusual patterns. This would assist in identifying red flags and strengthen both fraud control and detection.[108]

197. A word of caution is needed regarding the potential risks of "automation" and the over-reliance on built-in automated controls. Even the best automated controls can be circumvented through, for example, collusion, or simply if staff with various approving authorities do not know or do not pay sufficient attention to what they approve. While this problem also exists with more traditional and paper-based control functions, it is arguably more acute when approvals are made on systems that are of certain complexity, may lack user-friendliness and for which adequate training may not have been provided.

198. The implementation of the following recommendation is expected to enhance the effectiveness and efficiency of the organization's anti-fraud programme.

[108] Executive Committee of the High Commissioner's Programme, Follow-up on the recommendations of the Board of Auditors on the financial statements for previous years, EC/66/SC/CRP.4, para. 17.

Recommendation 10

The executive heads of the United Nations system organizations should ensure that proportionate fraud prevention and detection capabilities are an integral part of automation systems' functionalities, including automated activity reports and data-mining modules in their respective enterprise resource planning systems (ERPs).

H. Role of internal audit in fraud detection and control

199. All internal audit offices within the United Nations system have adopted the IIA International Standards for the Professional Practice of Internal Auditing, which outline the role of internal auditors in anti-fraud activities. They prescribe that internal auditors must have "sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization" (1210.A2). Furthermore, internal audit offices are expected to "evaluate the potential for the occurrence of fraud and how the organization manages fraud risk" (2120.A2) and auditors must "consider the probability of significant errors, fraud, noncompliance, and other exposures" when developing the objectives of each engagement (2210.A2). The head of internal audit must report periodically to management, including on "significant risk exposures and control issues, including fraud risks" (2060).

200. Notwithstanding the substantial role in fraud control that internal auditors are expected to fulfil, this review revealed that most United Nations system internal audit offices are focusing predominantly on compliance, assurance and advisory activities and, in most instances, do not necessarily devote focused attention to fraud control activities. Interviews also suggested that there is need for improvement with respect to the cooperation between internal audit and investigation offices, in particular through systematic and prompt cross-referral of cases whenever applicable (see chapter XI, section C below).

201. There is also room for audit offices in the United Nations system to become more proactive players in the fight against fraud. Proactive detection aims to identify suspicious activities ("red flags") by means of automated controls, targeted checks and monitoring, and to uncover potential fraud cases through proactive forensic auditing techniques and proactive investigations. Such activities include the search for patterns that indicate potential fraud in various databases and ERP-generated data sources, including the "mining" of logged system and user data and triangulating different data sources. For example, proactive identification of substantial fraud risks through the use of data and information technology-driven continuous auditing,[109] which a few United Nations organizations (e.g. UNOPS, UNFPA and WIPO) are currently implementing, is a feasible approach for internal audit offices to make the case to senior management for stronger anti-fraud control measures.

[109] Continuous auditing is defined by IIA as the automatic method used to perform control and risk assessments on a more frequent basis.

202. In their response to the questionnaire, many audit offices[110] indicated that they consider fraud risks as part of their standard engagement planning, including standard checklists. UNAIDS and WHO request all of their auditees to complete a fraud risk self-assessment as part of their engagement planning prior to undertaking any field mission. Other organizations, such as UNFPA, indicated that their audit offices refer "red flags" related to fraud risks to the investigators and vice versa, in line with their respective mandates. This practice, however, is not widespread. **As part of their internal risk assessments, internal audit offices should systematically include fraud risks in the preparation of their specific audit engagements.**

203. The review further revealed that most internal audit offices in the United Nations system have not made an overarching audit on the status of anti-fraud efforts of their respective organizations. **It is highly recommended that internal audit offices consider, if they have not already done so, the inclusion of an organization-wide performance audit of the effectiveness and measures taken by their organization's management to combat fraud, inclusive of anti-fraud policies, ethics policies, anti-fraud strategies and action plans and their implementation.**

VIII. FRAUD COMPLAINT MECHANISMS (PILLAR 5)

204. Fraud complaint mechanisms, such as whistle-blower hotlines and other available reporting channels, are the primary tool of uncovering fraudulent activities. They also provide a strong deterrence for staff and third parties to committing fraud when they know they may be discovered and reported. The review found that whistle-blowers alone are the reason for the uncovering of more fraud and corruption than all other measures of fraud detection combined. The finding is supported by similar statistics in the international community. As shown in a 2014 ACFE survey, on average more than 40 per cent of cases originate from tips received from whistle-blowers.[111] Tipsters and whistle-blowers are crucial in cases where fraud is committed through collusion and in sophisticated fraud schemes without paper trails, or cases that are very difficult to identify and gather evidence for, such as high-value fraud in procurement, grants and funds paid to implementing partners.

205. While United Nation system organizations have adopted whistle-blower policies and other fraud reporting mechanisms, many interviewees expressed concerns regarding the effectiveness of their implementation. The plethora of different reporting venues and the fragmentation of the reporting system were mentioned as the main obstacles to the proper reporting of suspected fraudulent activities. Furthermore, it was highlighted that third parties, such as vendors, implementing partners and beneficiaries, may not have information and access to whistle-blower hotlines and other reporting channels.

[110] These include WIPO, UNOPS, UNIDO, UNICEF, UNHCR, UNFPA, UNESCO, UNEP, UNDP, UN-Women, IAEA and FAO.

[111] ACFE, *Report to the Nations on Occupational Fraud and Abuse* (2014), p. 4.

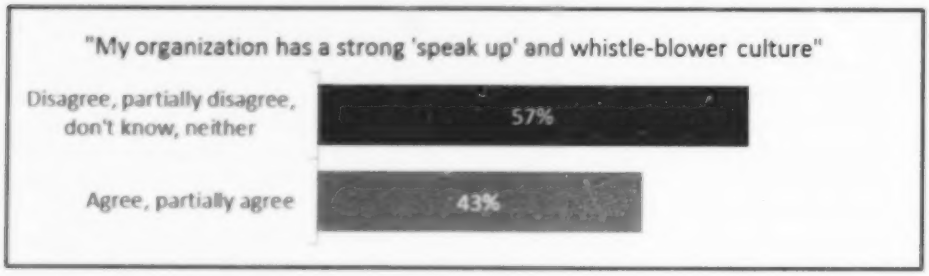
A. Whistle-blower policies

206. According to the standards of conduct for the international civil service, published by ICSC, the obligation to report fraud and the process of reporting need to be outlined clearly in the policies:

> *"International civil servants have the duty to report any breach of the organization's regulations and rules to the official or entity within their organizations whose responsibility it is to take appropriate action, and to cooperate with duly authorized audits and investigations. An international civil servant who reports such a breach in good faith or who cooperates with an audit or investigation has the right to be protected against retaliation for doing so".*[112]

207. The majority of United Nations organizations have adopted provisions that govern whistle-blowing and the "duty to report" fraud and other misconduct in line with the ICSC Standards; most organizations have gone further by adopting a dedicated policy for protecting whistle-blowers against retaliation.[113] **However, interviews and the JIU fraud survey suggest that not all United Nations system personnel are fully aware of their organization's policies or the duty to report in line with the ICSC standards. In fact, more than half of the respondents in the JIU fraud survey do not perceive a strong 'speak-up' and whistle-blower culture in their organizations (see figure 5).**

Figure 5: Whistle-blower culture


"My organization has a strong 'speak up' and whistle-blower culture"
Disagree, partially disagree, don't know, neither
57%
Agree, partially agree
43%

Source: JIU fraud survey.

208. Literature research and guidance provided by professional organizations indicate an emerging consensus on good practices related to whistle-blower policies. Box 4 below presents a non-exhaustive list of such practices.

[112] Report of the International Civil Service Commission (A/67/30), annex IV, para. 20.

[113] Examples of most recent work on whistle-blowing include policy updates by WHO in 2015 and the proposed revisions by the United Nations Ethics Office of the Secretary-General's bulletin ST/SGB/2015/21 on protection against retaliation for reporting misconduct. See also report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/70/361), p. 20.

Box 4: Good practices in whistle-blower policies (non-exhaustive)

- **Clear written provisions:** Clear and easily understandable language on whistle-blower provisions
- **Broadly available:** Readily available and well-publicized
- **Inclusive coverage of the definition of whistle-blower:** As broad as possible (staff, interns, volunteers, third parties, beneficiaries etc.)
- **Broad subject coverage:** Types of disclosures to include fraud, other types of misconduct and any disclosures in the public interest[114]
- **Clear roles and responsibilities:** Clear definition of who does what after a report has been made
- **Provisions on the reporting process:** Clear outline of the process and steps to follow
- **Allow for anonymous reporting:** Allow for anonymous reporting but also provide credible protection for the anonymity of whistle-blowers if requested
- **Provisions for protection against retaliation**

Source: JIU 2015, based on literature review.

209. Having clear policies that govern the anonymous or confidential reporting of fraud and other misconduct is considered good practice throughout the international community and the private and public sectors. The review found that the right to anonymous reporting and protection of the anonymity of whistle-blowers should they wish to come forward rank high among respondents to the JIU fraud survey and also among staff interviewed for the present report. While anonymity is promoted in the majority of the United Nations system organizations' policies, it should be noted that the exigencies of due process may occasionally trump the desire to maintain anonymity. An individual accused of misconduct also has the right to due process and defence. The accused must be afforded a fair opportunity to challenge testimony used against him or her in administrative, disciplinary or judicial proceedings. In certain cases such testimony may include that of a whistle-blower, who could in consequence be identified either expressly or by inference as the source of the original complaint. The United Nations Administrative Tribunal has expressed an opinion to that effect.[115] Notwithstanding the above the desire for

[114] See also commentary in UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons* (2015): "In law and policy the concept of 'public interest' allows judges and policy makers to consider interests that are at stake that are not necessarily represented in the specific case or matter before them. The flexibility is intentional to respond to new or different factors affecting the public interest according to the circumstances of each situation."

[115] United Nations Administrative Tribunal: "Obviously there are cases in which it is essential for the accused person to know the source of the allegation against him in order to enable him to challenge the honesty, reputation or reliability of a witness. There are cases in which a witness must be identified so as to afford 'due process' to a person with an alibi or a similar defence. In such cases the Tribunal is satisfied that the rights of an accused person to a fair hearing are superior to those of a person seeking anonymity. Under those circumstances the matter should not proceed unless there is disclosure of the identity of the accuser or witness as the case may be." (Judgement No. 983, Idriss (AT/DEC/983)).

anonymity and protection from retaliation should be respected and anonymity should be lifted only in extreme cases and with the consent of the whistle-blower.

210. **Without prejudice to due process rights of individuals accused of misconduct, it is recommended that good practice measures should be put in place to safeguard the anonymity or confidentiality of whistle-blowers. The results of the fraud survey and numerous interviews indicate that much more needs to be done to strengthen existing policies procedures and practices in this area.**

211. In addition to whether anonymous reporting is practised by the organization is the issue of whether reports received anonymously are treated in the same way as reports received from identified sources. Discriminating against anonymous reports may lead to the high risk that serious cases may go unreported. In the United Nations system, a few organizations (ILO, IMO, ITU and UNAIDS) do not offer the option of anonymous reporting through their whistle-blower hotlines. Such organizations should consider encouraging anonymous reporting combined with mechanisms to protect the anonymity of or confidentiality for whistle-blowers.

212. Another key aspect of an effective whistle-blower policy is to cover not only staff and other personnel, but to broaden the scope of application as much as possible in order to enable and encourage reporting by third parties as well, such as vendors and implementing partners. The majority of policies within the United Nations system in principle allow for reporting by third parties. Most United Nations system organizations, however, are not proactive in advertising and promoting the organization's whistle-blower hotline to parties external to the organization or in encouraging or seeking out third party reporting, which is crucial to uncover elaborate fraud schemes, collusion or fraud in distant locations where access may be impeded due to safety and security concerns.

213. **Not all United Nations system organizations make their whistle-blower provisions readily available on their external websites. A good practice followed by other multilateral institutions (i.e. the World Bank) is to advertise on their public website whistle-blower reporting mechanisms and specifically solicit reports from third parties.**

214. **Furthermore, it is good practice for contracts and legal agreements to include provisions for extending the duty to report fraud and other misconduct to contract employees, United Nations volunteers, interns and other non-staff, as well as vendors, suppliers and implementing partners.**

215. In addition to the "duty to report", some private and public sector entities encourage whistle-blowers to come forward through an incentive or rewards scheme. Such incentives could include financial (for example, in-grade promotions) or non-financial (such as public recognition) rewards, or other advantages and benefits granted for self-reporting, such as reduced sentencing in the case of implicated staff members. The United Nations Convention against Corruption, which has been ratified by the vast majority of Member States of the United Nations, contains some provisions to encourage persons who participate or participated in acts of corruption to supply information, including through "mitigating punishment" (art. 37 (2)) and "granting immunity" (art. 37 (3)). Within the United Nations system, some interviewees indicated that offering incentives to

whistle-blowers may be seen to conflict with the logic of the duty to report. However, while not suitable for every organization and depending on the particular strengths and weaknesses of the anti-fraud strategy in place, incentive schemes may be considered as an option to boost report intake.

216. The implementation of the following recommendation is expected to enhance the effectiveness and efficiency of the organization's anti-fraud programme.

Recommendation 11

The executive heads of the United Nations system organizations, if they have not already done so, should revise their whistle-blower policies with a view to adopting good practices, and extend the duty to report fraud and other misconduct to contract employees, United Nations volunteers, interns and other non-staff, as well as to third parties, including vendors, suppliers and implementing partners.

B. Whistle-blower hotlines

217. Whistle-blower hotlines[116] are the most common channel for tipsters to report suspected fraud and other types of wrongdoing. The United Nations Convention against Corruption contains provisions on whistle-blower hotlines that call for Member States to consider, inter-alia, "establishing measures and systems to facilitate the reporting by public officials of acts of corruption to appropriate authorities" (art. 8 (4)), and to "ensure that the relevant anti-corruption bodies referred to in this Convention are known to the public and shall provide access to such bodies, where appropriate, for the reporting, including anonymously, of any incidents that may be considered to constitute an offence established in accordance with this Convention" (art. 13 (2)). The same principles apply to the United Nations system organizations.[117]

218. The majority of the United Nations system organizations reviewed have established formal hotline mechanisms for reporting complaints of suspected fraud and other misconduct. In some organizations, however, such as ILO, IMO, ITU and UNAIDS, complaints can only be made in person, by regular mail, by e-mail, by fax, or through the ethics office.

219. Of those organizations that have hotlines, the majority administer them internally. A few organizations (UNDP, IAEA, UNWTO and UPU) have opted to contract out the administration to an external professional service provider.

220. Box 5 presents good practices in the international community that constitute benchmarks for implementing effective whistle-blower hotlines.

[116] Sometimes these are also referred to as "tipster" or "speak-up" hotlines.

[117] UNODC "The Institutional Integrity Initiative", p. 60. See also the recommendation by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in A/70/361 to "provide effective and protective channels for whistle-blowers to motivate remedial action" (para. 64).

Box 5: Good practices for whistle-blower hotlines (non-exhaustive)

- **Accessibility to third parties:** Accessible to contractors, vendors, beneficiaries and others
- **Availability 24/7:** Accessible around the clock
- **Toll-free phone calls:** Accessible via a toll-free/collect call telephone number
- **Multilingual:** Available in the languages of major stakeholder groups
- **Anonymous reporting:** Whistle-blowers should not be required to identify themselves
- **Multi-channel accessibility:** Accessible by phone, e-mail, through a website and in person
- **Encrypted e-mail/webpage:** E-mail/webpage communication should be encrypted in order to protect anonymity

Source: JIU compilation based on good practices.

221. As part of this review, JIU assessed existing whistle-blower hotlines in the United Nations system against the benchmarks outlined above. Most organizations have implemented the majority of those benchmarks. However, it was noted that hotlines are not toll free in some organizations, issues of anonymity arise where e-mail systems are used and, in a number of organizations, hotlines and related guidance are not available in multiple languages.

222. Another good practice is to offer a proxy communication channel for anonymous whistle-blowers. Such a communication channel has the dual function of offering investigators an opportunity to follow up with the anonymous person for inquiries following the initial report, as well as to communicate subsequent outcomes to the whistle-blower while maintaining anonymity. The Global Fund, for example, has a PIN-activated electronic communication channel for that purpose and UNESCO recommends whistle-blowers who wish to remain anonymous contact the investigation office via an Internet-based, free e-mail address.[118]

223. Some interviewees indicated that hotlines should also offer an alternative route for reporting for cases involving senior management. Such a route could, for example, constitute a whistle-blower reporting line to the audit committee, or another channel, as established by the organization. The recommendation of a previous JIU report[119] that called for regular referrals of investigation cases of executive heads to a separate and independent entity is hereby reiterated.

224. **It is recommended that United Nations system organizations review the arrangements for their whistle-blower hotlines with a view to adopting the good practice benchmarks outlined in box 5. Organizations that have not put in place a whistle-blower hotline are encouraged to do so in accordance with these benchmarks.**

[118] See UNESCO webpage www.unesco.org/new/en/unesco/about-us/how-we-work/accountability/internal-oversight-service/report-fraud-corruption-or-abuse/ (accessed on 7 December 2015).

[119] The investigations function in the United Nations system (JIU/REP/2011/7), paragraph 36.

225. In certain United Nations system environments, efforts to advertise and promote the organization's whistle-blower hotline should be also extended to beneficiaries, including by facilitating their use by offering services in local languages in case of large-scale operations, offering free telephone services or complaints boxes, for example in refugee camps, and distributing information about the hotline among beneficiary populations. For example, UNHCR has some of these measures in place, including notices in the leaflets distributed to beneficiary populations warning beneficiaries of fraud involving UNHCR services and providing information on where to refer their complaints in cases of suspected fraud.[120] These are effective and cost efficient measures for receiving indications and information from the field on any possible fraudulent acts.

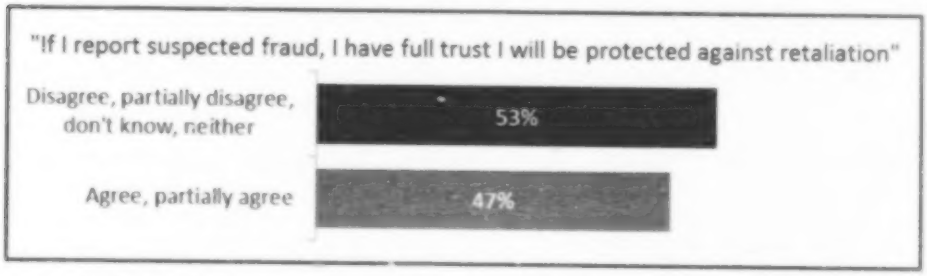
226. **As applicable to certain United Nations system organizations, it is recommended that concerted efforts should be made to make whistle-blower hotlines accessible to beneficiaries, in addition to other partners with whom the organization has programmatic links.**

C. Protection against retaliation

227. The protection of whistle-blowers against retaliation is vital to build and maintain long-term confidence among staff to report fraud and to create and maintain a speak-up culture. In order to encourage whistle-blowers to report, organizations must have provisions and procedures to address retaliation complaints and remedy proven retaliation. While the whistle-blower policies of the United Nations system may include such provisions, their success depends on how these provisions are effectively implemented and the trust of staff at large in the policies for protection against retaliation.

228. The JIU fraud survey results revealed that more than half of the respondents are not certain they would be protected against retaliation if they reported fraud. The above responses show that much needs to be done to promote and inform staff about the organization's whistle-blower and anti-retaliation mechanisms.

Figure 6: Protection against retaliation


"If I report suspected fraud, I have full trust I will be protected against retaliation"
Disagree, partially disagree, don't know, neither
53%
Agree, partially agree
47%

Source: JIU fraud survey.

229. Fear of retaliation — whether substantiated or perceived — was also brought up by interviewees as a matter of serious concern. Integrity and ethics surveys and

[120] See, for example, UNHCR, "Service Guide for Syrian Refugees valid as of January 2015".

reports, conducted internally by some United Nations system organizations, indicate that whistle-blower reporting and protection against retaliation rank high among problem areas reported by staff. For instance, in one organization, the ethics office noted that potential complainants were aware of the policies and mechanisms, but were reluctant to use them because of the fear of reprisal. This is in line with responses received in the context of a 2012 global staff survey of the same organization that reflected "the fears of retaliation and the lack of confidence that those who do report misconduct will be protected from retaliation could hold staff back from speaking up and reporting misconduct in the first place". In another organization, the oversight office and the ethics office indicated in their reports that "feedback received during ethics awareness workshops indicate that staff members remain concerned about the possibility of workplace retaliation". In yet another organization, the ethics office report states that "staff members raised their fear or frustration to speak up", despite the organization's specific whistle-blower protection policy. The ethics office report of yet another organization stated that "it is noteworthy that there is an increasing number of inquiries that are reported collectively, by a group of employees, or by unknown or anonymous sources".

230. A Special Rapporteur report also found that existing provisions for the protection of whistle-blowers contain certain loopholes and exceptions in their coverage in United Nations system organizations.[121] In many cases, the mechanisms in place, while well-intentioned, lack real independence and effectiveness. As long as internal reporting channels require implementing actions by multiple individuals in the organization's management, they will fail to enjoy the credibility that comes with independent review.[122] This has potential deterrent effects in that those with knowledge of fraud or presumed fraud may not be as forthcoming. Additionally, those that come forward may find themselves retaliated against without adequate recourse.

231. Ethics offices throughout the United Nations system face the challenge of "weeding out" actual cases from those related to workplace and performance issues. Several interviewees also pointed out that sometimes retaliation claims are used under false pretences to prolong employment. The Ethics Office of the United Nations, since its 10 years in existence (2006-2015), following prima facie review and subsequent investigation by OIOS, made a final determination of retaliation in only four cases.[123] According to the Secretariat's Ethics Office, the anti-retaliation policy is frequently "utilized as a grievance and labour dispute mechanism",[124] which reflects the experience of other ethics offices within the United Nations system. At the time of this review, the Secretariat was revising its anti-retaliation policy, in accordance with emerging global best practices, aiming to refocus on protecting whistle-blowers who reported allegations or cooperated with investigations of wrongdoing that posed substantial harm to the interests, operations or governance of the organization. It is expected that the new policy would limit the intake of unrelated reports.

[121] See, Special Rapporteur on the promotion and the protection of the right to freedom of opinion and expression (A/70/361), paras. 51-69.

[122] Ibid., para. 55.

[123] Reports on the activities of the Ethics Office, A/66/319, A/67/306, A/68/348, A/69/332 and A/70/307.

[124] Ethics Office of the United Nations Secretariat, 2015.

232. As discussed, good practice suggests that, in order to give credibility to the claim of protecting the anonymity or confidentiality of whistle-blowers, the information that whistle-blowers provide must be treated sensitively and a number of safeguards put in place. Within the United Nations system, such measures include: securing premises for the office handling whistle-blower reports; special access restrictions for records (locked cabinets etc.), including special provisions for electronic files, for example separate server or electronic firewalls. Confidentiality requirements for all persons with access to sensitive information are necessary. The requirement to keep information confidential should not only extend to staff handling whistle-blower cases, but also to other persons with access to privileged information, such as information technology personnel, witnesses etc.[125]

233. Awarding interim relief — measures aimed to temporarily avert further harm — to whistle-blowers who fear retaliation is a good practice implemented by the United Nations Secretariat, UNDP, UNHCR, UNWTO, UNESCO, FAO, WFP and WHO. Such measures could include being transferred to a different department or being assigning a different supervisor. A number of interviewees indicated that awarding interim relief measures raised significant administrative difficulties in practice, which need to be addressed with urgency by the management to ensure efficient implementation of anti-retaliation policies. Some interviewees also strongly suggested that interim relief measures should only be taken with the consent of the whistle-blower so that they are not used for disguised retaliatory purposes.

234. While most organizations have in place provisions for the protection of staff members, the same is not always the case for non-staff engaged by the United Nations system, such as consultants, special services agreement holders, United Nations volunteers, interns or seconded personnel. A number of organizations have established specific provisions to extend the protection against retaliation measures in principle to persons in the non-staff category, who have a contractual link to the organization. For instance UNDP, WHO, UNESCO, IMO and UNRWA explicitly cover non-staff members, such as volunteers, interns, contractors and consultants under their anti-retaliation policies. The United Nations Secretariat in its policy (ST/SGB/2005/21) expressly extends protection against retaliation not only to staff members who report misconduct or otherwise engage in an activity protected under the policy, but also to certain categories of non-staff members, namely interns and United Nations volunteers.

235. **It is recommended that United Nations system organizations extend and apply appropriate whistle-blower protection measures against retaliation, not only to staff members but also to various non-staff categories, including personal services contractors, volunteers and interns, as long as there is a contractual link with such individuals.**

236. Absent from many anti-retaliation frameworks by United Nations organizations reviewed are provisions to mitigate conflicts of interests arising when wrongdoing is reported to have taken place by either an ethics office or an investigation function. For example, during 2010/2011 the United Nations Secretariat's Ethics Office faced a case of prima facie retaliation by the

[125] Please see also section A of the present chapter.

investigation function, which was addressed on an ad hoc basis by establishing an alternative investigation panel. Some organizations have addressed this issue by amending their policies to that effect that for cases of potential conflict of interest, the head of the ethics office can refer the review to be done by an alternative reviewing body.

237. A number of international bodies have established policies that are considered good practices in the protection of whistle-blowers against retaliation.[126] While some of these practices are already followed by United Nations system organizations, there is room for a thorough review of such policies to see if and how they can fit in the current business environment and the needs of each organization. For example, a good practice is to provide comprehensive coverage by whistle-blower policies, including for "spillover retaliation" that affects persons presumed to be whistle-blowers. Policies in line with good practices also provide for a guarantee of the confidentiality of the whistle-blower, place the "burden of proof" to assess potential retaliatory action on the employer once a prima facie case has been established and grant access to a formal justice systems. Furthermore, such policies provide for feedback to be given to whistle-blowers on the outcomes of a report and provide for specific penalties and/or disciplinary action to be taken against those that engaged in retaliation.

D. Multiplicity of reporting — centralized v. decentralized intakes

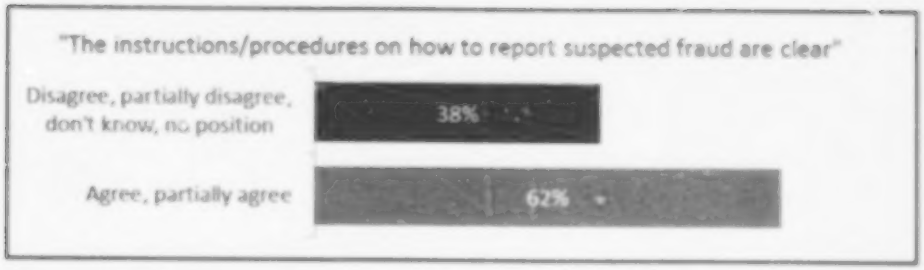
238. The review revealed that organizations have different approaches in managing the intake process of complaints, in conducting preliminary assessments of fraud and other complaints of misconduct, in determining prima facie cases of alleged retaliation, and in assigning the conduct of investigations to the responsible unit. In a number of organizations, the investigation function (or oversight office) is designated as the main entity entrusted with receiving fraud allegations, managing the hotline, and subsequently conducting the investigations. However, in most organizations, allegations of suspected fraudulent behaviour (and other misconduct) are also reported through various channels, such as through direct supervisors and senior management, human resources departments, ethics offices, executive heads and others.

239. The existence of multiple channels in reporting fraud and other misconduct leads to a lack of clarity on how they relate to each other, which types of complaints are to be received by what office, and how cross-referring allegations and/or informing on actions taken should be done. Furthermore, in many cases, the rules for preliminary investigations and assessment of allegations and pre-screenings are not clear or formalized. In the JIU fraud survey, close to 40 per cent of respondents

[126] UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons*; Transparency International, *Whistleblower Protection and the UN Convention against Corruption* (2013); OECD, *Whistleblower Protection: Encouraging Reporting* (2012); Council of Europe, recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the Protection of whistleblowers; G20, *Study on Whistleblower Protection Frameworks, Compendium of Best Practices and Guiding Principles for Legislation* (2011); U4 Anti-Corruption Resource Centre (2008), "Making whistleblower protection work: elements of an effective approach"; A/70/361.

indicated that "instructions and procedures on how to report suspected fraud" were either unclear or unknown (see Figure 7 below).

Figure 7: Fraud reporting


"The instructions/procedures on how to report suspected fraud are clear"
Disagree, partially disagree, don't know, no position
38%
Agree, partially agree
62%

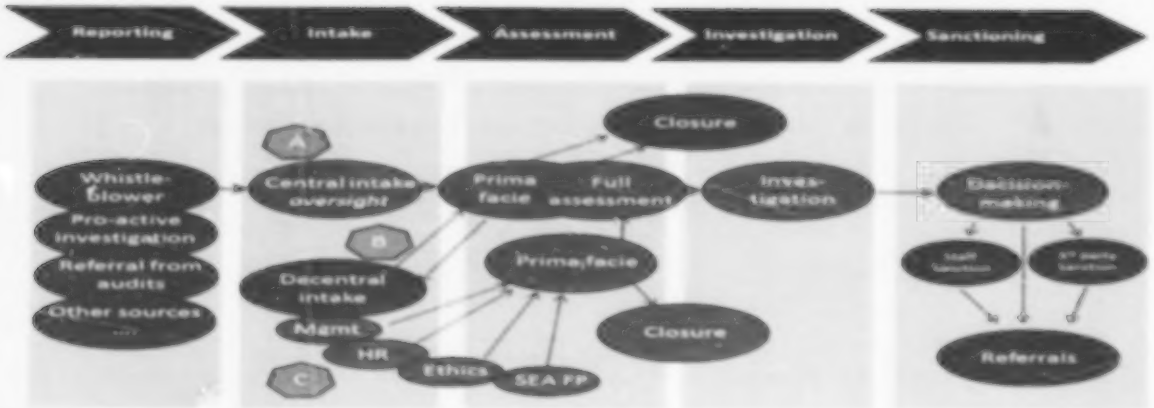
Source: JIU fraud survey.

240. **The lack of clarity on how to report fraud, the fear of retaliation, and the lack of trust on the procedures to be followed may prevent and deter whistle-blowers from reporting allegations and, as such, contribute to underreporting of fraud. A total of 47 per cent of responders to the JIU fraud survey brought up these three factors as the main reason for not coming forward with reporting fraud to a higher authority.** In addition to creating confusion, multiple reporting venues may also lead to errors of judgment and delays when, for example, fraud allegations are referred to the wrong office. Furthermore, the absence of a single point of contact for reporting fraud cases also means that allegations will not be consistently evaluated in the first instance.[127] Many interviewees acknowledged that clear procedures for sharing all allegations and the results of preliminary investigations/assessments with the investigation function would allow the organization to have an understanding of the range of allegations within the organization, including fraud, and how they are being addressed.

241. The organizations reviewed for the present report fall, broadly, into one of two main categories (centralized and decentralized), as illustrated in figure 8 below. A number of organizations have a central intake mechanism, which is usually the oversight office (or investigation function) that conducts a prima facie assessment of all allegations received and, if warranted, either conducts a full investigation or refers the case to another responsible office. In other organizations, the intake is decentralized and, accordingly, allegations and complaints can be received by a number of different units that in turn refer the cases to the respective oversight function or prima facie assessments are conducted at the decentralized level with optional referral to the oversight office.

[127] A/69/5 (Vol. I), para. 145.

Figure 8: Fraud reporting



Source: JIU, 2015.

242. **A central intake system for all allegations (designation A in figure 8)** within the internal oversight office (or investigation function) is an approach adopted in some United Nations system organizations to address this issue (e.g. IMO, UNFPA, WHO and UNHCR). A central intake mechanism has the benefit of ensuring a "complete picture" by allowing for a coherent and consistent review and preliminary assessment of all allegations and complaints at a single entry point, applying the same process for all allegations. In doing so, it permits the prioritization of cases and effective and efficient use of limited resources for follow-up investigations, focusing on a risk-based approach to addressing and investigating fraud allegations. It also prevents possible conflicts of interest, as the pre-assessment and decision on opening an investigation or not is done by an independent entity, not by an entity closely connected to the allegation. Furthermore, a central intake facilitates the completeness of reporting of fraud and presumptive fraud to external auditors.[128]

243. It should be noted, however, that, while in a central intake system the hotline reporting and the follow-up is assigned to the investigation function, complaints about the protection against retaliation (see section D below) are handled, as a matter of good measure, by the ethics office, which conducts a prima facie assessment and then forwards cases to the investigation function. Once the investigation has been concluded the report is reviewed by the ethics office, which makes a recommendation to the executive management on the appropriate action/measure to be taken. In UNRWA and IMO, both the ethics office and the investigation function are located under the same directorate. Separating the two functions, in these organizations, is desirable to avoid any potential conflicts of interest. In some organizations, such as UNDP and UNFPA, while the oversight offices are the primary intake hubs and operate a hotline for fraud and other types of misconduct, the ethics offices also operate an ethics helpline in recognition of the need for the ethics offices to provide ethics advise and be the focal points for

[128] See also A/70/284, para. 89 (concerning the United Nations Secretariat).

addressing office-related ethics issues. Similarly in the United Nations Secretariat, the ethics office operates a helpline to provide confidential ethics advice.

244. On the downside, a centralized intake can overload the system, in organizations with limited resources, by the high volume of unrelated reports received centrally, which then need to be referred elsewhere. For example, during interviews, it was mentioned that, of the calls received by the UNHCR whistle-blower hotline, a large number were related to refugee protection issues unrelated to misconduct and/or fraud.

245. **A decentralized intake mechanism (designation B and C in figure 8)** involves intake by multiple parties and requires very clearly delineated categories and definitions of the various types of misconduct. In this scenario, the different categories of misconduct need to be clearly understood by prospective whistle-blowers, in order that they can address themselves to the appropriate reporting channel. Such decentralized arrangements are more common in organizations with a strong decentralized structure, with multiple regional and country offices. Typically, allegations of possible fraud are brought to the attention of the immediate supervisor, who in turn refers the case to the head of office or representative. Then, depending on the preliminary assessment, the allegation may or may not be reported to headquarters, i.e., the case may be handled and settled at the country or regional level. In some organizations, there are units at the field level entrusted with receiving and handling disciplinary cases on their own, including those related to fraud allegations.

246. In the United Nations Secretariat, there are two categories of cases for investigation, category I which includes serious fraud, misconduct, criminal acts etc., and category II, which includes personal matters, traffic-related incidents, simple thefts, staff disputes etc. Category I cases are normally handled by OIOS and category II cases by other entities, such as OHRM, heads of offices, conduct and discipline units (such as in the Department of Peacekeeping Operations/Department of Field Support). As indicated by IAAC, and further confirmed by this review, these distinctions have not been clear in all instances and cases have been referred back to management when they should have been handled by OIOS, and vice versa.[129] Furthermore, it appears that that there is currently no office or entity within the Secretariat that keeps track of all investigations under way throughout the Secretariat's domain. While OIOS may hold this responsibility, given that not all cases originate from investigations initiated or recommended by OIOS, there remains a need to at least monitor the statistics on all investigations under way and the recommended disciplinary actions.[130] Interviews conducted for this review indicate that other United Nations system organizations are faced with similar challenges.

247. Finally, a fully decentralized intake arrangement coupled with prima facie assessments to be conducted at the decentralized levels may be less burdensome on the workload of oversight office, but has a number of disadvantages. Among them, the potential conflict of interest within decentralized intake entities, a lack of

[129] Activities of the Independent Audit Advisory Committee for the period from 1 August 2013 to 31 July 2014 (A/69/304), para. 69.

[130] See A/70/5 (Vol. I) and Corr.1, para. 103.

centralized information on fraud prevalence and trends across the organization and insufficient documentation of cases. Together, these characteristics may render the decentralized intake model with prima facie assessment unsuitable to a number of organizations.

248. It should also be mentioned that, in some organizations, allegations of fraud (and other misconduct) are handled by ad hoc panels/committees at different levels of the organization. For instance, at the United Nations Environment Programme (UNEP), which follows the United Nations rules and regulations, the review and determination of a reported complaint is done internally and a decision is made if the case warrants further investigations. If the case is considered high risk and meriting investigation, it is referred to OIOS of the United Nations Secretariat. If UNEP considers the case to be low risk, it establishes an ad hoc panel to investigate the matter. Conversely, when an allegation of misconduct is reported by a UNEP staff member directly to OIOS, OIOS determines whether it warrants an investigation, at which time, if the case is considered low risk, the matter is referred back to UNEP for investigation by an ad hoc panel. UN-Habitat follows a similar practice.

249. Regardless of the specific model that organizations have put in place, what emerges from the review is the crucial need for the existence of a central authority for intake, processing and investigating of complaints and providing a reliable depository of information on fraud-related offences. It is common practice for the investigation function to be the central point of entry and depository for recording fraud-related cases including for allegations received through various channels and outcomes of preliminary assessments, and deciding on whether (or not) to open a formal investigation. The investigation function is expected to carry the responsibility for quality assurance of the preliminary assessment process and for providing support to management on follow-up actions and mitigation measures, such as disciplinary measures, sanctions, administrative/management recommendations and referrals of cases to national law enforcement. A single intake mechanism for reporting fraud and other misconduct is considered good practice, and as it is also suggested by the BOA[131] and reiterated by the IAAC,[132] it should be the appropriate mechanism for certain organizations in the United Nations system.

250. The implementation of the following recommendation is expected to enhance the effectiveness and efficiency of the organization's anti-fraud programme.

Recommendation 12

The executive heads of the United Nations system organization, if they have not already done so, should implement the good practice of establishing a central intake mechanism for all fraud allegations in their respective organizations. In the interim, for organizations with decentralized intake mechanisms, immediate action should be taken to: (a) establish an obligation for decentralized intake units to report to a central authority any allegations received, ongoing cases under investigation and closed cases, indicating the action taken; and

[131] Financial report and audited financial statements for the biennium ended 31 December 2013 and report of the Board of Auditors, A/69/5 (Vol. I), para. 148.

[132] A/70/284, para. 89.

(b) establish formal intake procedures and guidelines, including: clear criteria for the preliminary assessment, the official, office or function authorized to make the assessment, the process to be followed and the arrangements for reporting on the results of the preliminary assessments.

IX. INVESTIGATIONS (PILLAR 6)

251. Investigations are key to a robust anti-fraud programme and crucial to effective fraud control. They are not only necessary as a reactive (and sometimes proactive) measure in fraud detection, but they have a significant preventive function, by deterring potential fraudsters from committing fraud. The main objective of a fraud investigation is to collect evidence relating to specific fraud allegations to determine the facts relating to the case and to assist management in deciding what action should be taken if the allegations are proven true through a professional investigative process.

252. Most United Nations system organizations have in place professional investigative teams as part of their oversight offices, with the smaller organizations relying more on ad hoc availability of investigative know-how among their internal auditors or through external consultants and referral of cases to investigative offices of other United Nations system organizations.

253. The following sections address selectively areas of the investigation function relevant to supporting an effective anti-fraud programme. They should be read in conjunction with previous JIU reports that have covered the investigative function in detail (JIU/REP/2011/7 and JIU/REP/2000/9).

A. Timeliness, capacity of and quality of investigations

254. The adequacy of resources and capacity of the investigation function has been the subject of past reports and ongoing reviews by the oversight community. These include reports by the JIU, the IAAC, the BOA, as well as peer reviews at some organizations.[133] While the investigation function challenges are of a broader nature in reference to the scope of the present review, certain aspects of special interest on the subject of fraud are highlighted below.

Timeliness and capacity of investigations

255. A number of interviewees in management positions but also staff at large felt that investigations in the United Nations system take too long. Investigators reported that complex fraud related investigations, i.e. in cases of collusion or fraud committed by third parties, may take an average of 12-18 months[134] and some even longer. In addition, the investigation process is only the first step and, if a case is substantiated, the investigation report will be reviewed by the management to determine the disciplinary and other corrective action. This follow-up process by the

[133] See e.g. JIU/REP/2000/9, paras. 55-70; A/70/284, paras. 63-66.
[134] See A/69/304, para. 53.

management takes on average 4-8 months. Usually, the longer an investigation the more difficult it may become to secure, collect and establish the necessary evidence.

256. In cases where the disciplinary decision and measure is appealed by staff members, several months of proceedings may follow at the United Nations system tribunals[135] as part of the process of the internal administration of justice.

257. **Many interviewees indicated that the long and protracted life cycle of the process, including the investigation, the disciplinary process follow-up and the tribunals promote a sense of impunity among fraud perpetrators in the United Nations system. It results in possible perpetrators not being deterred to commit fraud, and staff not inclined to report fraud,[136] as they believe, rightly or wrongly, that the organization is not disposed towards follow-up action or the perpetrator may not be punished even when sufficient evidence is present.** This is in line with the responses received through the JIU fraud survey, as displayed in figure 9, chapter X below. The results of other relevant surveys, such as the United Nations integrity survey conducted by the ethics office in 2014, show similar perceptions.

258. **Recommendations made by various oversight bodies[137] in the United Nations system that organizations address on a priority basis the problem of extended durations of investigations are hereby reiterated.**

259. **Reference is also made to the suggestions made by a number of investigation offices interviewed that, inter alia, appropriate resources should be provided by management and the legislative and governing bodies to address the issue of investigative capacity, taking into account the organization's fraud (and other misconduct) risks and exposure.**

260. It should be noted that, at the United Nations Secretariat, the increased emphasis on investigations involving major fraud, especially fraud by implementing partners, led to a donor government agreeing to fund an OIOS fraud investigation team, composed of three professional and one general service staff member based in Nairobi, for a period of four years. This is a commendable effort on the part of the donor that may alleviate some of the resource-related challenges that the investigative function is facing.

261. The implementation of the following recommendation is expected to enhance the effectiveness and efficiency of the organization's anti-fraud programme.

[135] United Nations Dispute Tribunal, United Nations Appeal Tribunal and the ILO Administrative Tribunal.

[136] See also Activities of the UNDP Ethics Office in 2014 Report of the Ethics Office (DP/2015/23), para. 61.

[137] See e.g. JIU/REP/2000/9, paras. 55-70; A/70/284, paras. 63-66; Voluntary funds administered by the United Nations High Commissioner for Refugees: financial report and audited financial statements for the year ended 31 December 2012 and report of the Board of Auditors (A/68/5/Add.5); A/69/304, para. 53; A/70/284, paras. 63-66.

Recommendation 13

The executive heads of the United Nations system organizations, in consultation with the audit advisory committees, should ensure that the investigation function of their respective organizations establishes key performance indicators for the conduct and completion of investigations, and has adequate capacity to investigate, based on a risk categorization and the type and complexity of the investigations.

Quality of investigations

262. Interviewees indicated that the quality of investigations, i.e. adherence to due process and professional practices, had been subject of criticism from the judges of the United Nations tribunals. The situation varies from organization to organization. Some organizations mentioned that the proportion of successful cases put forward by management has increased over the past years. Others indicated that a number of cases are being successfully appealed due to the quality, or lack thereof, of the underlying investigation. Yet, others mentioned that cases were closed by their legal offices, which had judged the cases could not withstand the scrutiny of appeals. No specific statistics or data were made available to the Inspectors to substantiate any of the above cases. Therefore, clear conclusions could not be drawn as to whether disciplinary cases were closed due to issues of poor quality of investigations and/or other factors.

263. Similarly, in the case of the United Nations, IAAC in its 2014[138] report examined the question of whether the current investigation function in the Secretariat was measuring up to the new United Nations justice system, comprising the United Nations Dispute Tribunal and the United Nations Appeals Tribunal. IAAC concluded that although both the OIOS and non-OIOS investigators fared relatively well at the tribunal level, investigations conducted by OIOS tended to perform slightly better.[139]

264. At the same time, the IAAC report also noted that looking at cases that ended up in the tribunals alone did not tell the whole story, as management said that it sometimes decided to close cases without disciplinary action, partly because it believed that such cases would not hold in the face of the current justice system.[140] Also IAAC was informed by management 'that the current investigation process in the Secretariat was not measuring up to the new, professional justice system, since, in addition to OIOS (who is the only body with professional investigators), ad hoc panels made up of heads of offices and departments, the Department of Safety and Security, special investigations units in peacekeeping missions and so on, were involved in the investigation process, and hence most of the investigations conducted by these ad hoc parties are carried out by non-professional investigators."[141]

[138] A/69/304.

[139] A/69/304, para. 66.

[140] A/69/304, para. 67.

[141] A/69/304, para. 63; see also A/70/284, paragraphs 63-66; see also General Assembly resolution 70/111, op. 14-18 concerning the Activities of the Office of Internal Oversight Services, and op. and 4 related to Activities of the Independent Audit Advisory Committee.

265. Many investigative offices interviewed, as well as legal offices, mentioned the challenges faced with regard the "standard of proof" required by the United Nations tribunals. Following a decision by the United Nations Appeals Tribunal in October 2011 that required the establishment of "clear and convincing evidence" rather than the previously applied standard of "preponderance of evidence", additional exigencies as to the quality of investigations are now required.[142] As explained by interviewees, this new level of proof is higher than the ones used prior to 2011, and in practice extends nearly to an equivalence of the level of proof used in criminal proceedings in many jurisdictions, which is "beyond reasonable doubt". Reportedly, this puts additional requirements on the depth and quality of the investigation. It should be noted that the World Bank routinely applies a lower level of proof ("more likely than not") to the evidence collected, which has the residual effect of reducing the length of investigations and the resources required.

266. Lack of and flaws on documentation are especially highlighted in tribunal judgments during the internal administration of justice proceedings, where some cases have been dismissed due to inappropriate documentation.[143]

267. Referral of cases to national law enforcement authorities is a particularly relevant and sensitive matter. Since the investigations conducted by the United Nations system are administrative and not criminal in nature, investigation reports and evidence collected may not be adequate for the national proceedings; hence in such cases additional evidence has to be collected causing extensive delays before it is presented to national authorities. Please refer to chap. X, sect. B. and recommendation 14 below on the issue of referrals.

B. Investigations of third parties and joint investigations

268. Investigations of third parties in general and in particular fraud investigations of implementing partners (NGOs and government entities), come with additional challenges and problems.

269. As noted in chapter VII, section F, one aspect is the need for extending the mandate of oversight offices over third parties and their subcontractors, including robust anti-fraud clauses in memoranda of understanding, contracts and other legal instruments.

270. Additional issues may arise in cases where the (implementing) partner is a government entity. Owing to legal and political considerations and related issues, the possible conduct of investigations of such partners is remote and comes with additional particularities and challenges. Not all partner memoranda of understanding and agreements reviewed contain provisions on these issues or clauses to this effect. Interviewees indicated that the most likely recourse for such cases would be the national audit office of the particular country, but referrals to such bodies are the exception rather than the norm.

[142] See A/70/5 (Vol. I) and Corr.1, para. 101.

[143] See, UNDT/2011/096, referenced in OHRM (2011), *Lessons Learned from the Jurisprudence of the System of Administration of Justice: A guide for managers*. The periodic reports of the Internal Justice Council may serve to further illustrate this situation; the latest report is the report of the Secretary-General on administration of justice at the United Nations (A/70/187).

271. However, the MDBs, such as the World Bank and the Inter-American Development Bank, have concluded cooperation agreements with national law enforcement authorities that outline the modalities in conducting and cooperating in investigations. These types of investigations are considered parallel or simultaneous investigations. The modalities of cooperation are outlined in the respective memorandums of understanding concluded between the MDBs and the respective national law enforcement authorities of the countries concerned, which also include clauses on confidentiality, allocation of work among the parties etc.

272. MDBs have also engaged in directly signing memoranda of understanding with other multinational investigative bodies, such as OLAF of the European Union in conducting investigations. Similar agreements have been concluded by OLAF with a number of United Nations system organizations (at the time of writing the present report, signed with UNDP, WFP and UNOPS, and in discussion with FAO and the International Fund for Agricultural Development). These are considered administrative cooperation arrangements, allowing for the opportunity to coordinate investigations, depending on the willingness of both entities to conduct such investigations and/or share information among the parties concerned.[144]

273. At the United Nations system level, UN-RIS has drafted a cooperation agreement on joint investigations[145] to be used as a template for similar arrangements among United Nations system organizations. This commendable agreement follows the template agreement for joint audits as endorsed by the Representatives of Internal Audit Services of the United Nations Organizations (UNRIAS), while taking into account the specificities and particular requirements of investigations. The agreement intends to formalize the existing cooperation on investigations among the United Nations organizations, which to date has been on an ad hoc basis. Emphasis is on cases of jointly funded projects, where there is great demand for a better coordinated approach based on best practices and a formal framework for cooperation.

274. **It is recommended that United Nations system organizations, in particular those which have large programme activity with implementing partners, should adopt the cooperation agreement on joint investigations as endorsed by UN-RIS.**

[144] According to the template administrative cooperation arrangements used, the cooperation between the partners usually includes the following activities: exchange of information; operational assistance; joint or parallel investigations; technical assistance; access to information systems and databases; strategic analysis; and training and staff exchange.

[145] UN-RIS formally adopted this agreement during its virtual meeting on 2 December 2015, following its consideration at the UN-RIS annual meeting in Montreux, Switzerland, on 29 September 2015.

C. Proactive fraud investigations

275. In contrast to "reactive investigations", which are instigated in response to allegations, reports or incidents, "proactive" fraud investigations are "investigations [that] aim to identify and control an existing (but yet unidentified) risk of fraud or financial irregularity".[146]

276. A number of the organizations reviewed indicated that they conduct at least some basic form of proactive investigations. However, the emphasis in most organizations remains clearly on reactive investigations. Consequently, in preventing and detecting fraud, most United Nations system organizations rely heavily on the effectiveness of internal controls, fraud reporting and whistle-blower systems. As discussed, these systems are not necessarily as robust in all cases as they should be (see chapters. VII and VIII above).

277. Many interviewees suggested that capacity and resource constraints are the two main obstacles to proactive investigations. The reactive approach to fraud reportedly absorbs nearly all investigation resources and very little is allocated to pursue more preventive and proactive measures against fraud. Some oversight offices indicated they would consider allocating considerable resources to preventive activities provided there was adequate coverage of ongoing reactive investigative work.

278. OIOS within the United Nations Secretariat has a specific mandate for proactive investigations, according to the Secretary-General's bulletin[147] that established OIOS. Recently, the OIOS investigations division established the dedicated Fraud Risk Unit to focus on fraud in high-risk operations through cooperation with the Internal Audit and Inspection and Evaluations Divisions of OIOS. This is a commendable effort and there are high expectations that these and similar proactive efforts will lead to improved fraud detection and deterrence.

279. At WFP, the proactive integrity review is a new initiative of the investigation function, which is based on a fraud risk assessment of higher-risk business processes or operations at all levels of the organization. This is a tool that examines WFP business processes or operations, to ensure that funds and assets are being utilized for their intended purposes and, in doing so, to assess their susceptibility to fraud corruption and/or other wrongdoings. As indicated by WFP, the review is not an investigation — which has the main objective of determining whether specific allegations can be substantiated — but rather it has broader objectives: to examine whether a business process or operation might suffer from fraud or corruption ("red flags"); and to assess how large the problem may be and to identify areas for follow-up and intervention, including identifying mitigation measures.[148]

280. UNDP has implemented a "proactive investigation model" that establishes the level of potential fraud risk in each country office in order to identify high-risk offices. The risk assessment process for proactive investigations consists of three stages: (a) identifying risk factors, establishing a rating scale, and assigning weights

[146] UNDP, Policy against Fraud and Other Corrupt Practices, para. 4.3.

[147] Establishment of the Office of Internal Oversight Services (ST/SGB/273), para. 17.

[148] WFP, annual report of the Inspector General, WFP/EB.A/2015/6-F/1, annex V "Charter of the Office of the Inspector General", paras. 18-19.

to risk factors; (b) risk ranking of country offices; and (c) identifying specific areas within a country office to be investigated.

281. UNHCR has created a new senior intelligence analyst post to strengthen data-mining capabilities with a view to identifying more cases proactively. Similarly, UNFPA has a dedicated data analyst working on continuous auditing who also contributes to proactive investigation work.

282. The need to have a more preventive and proactive approach to investigation work complementing reactive investigations has been highlighted in previous JIU reports.[149] It should be noted that the advantages of strengthening preventive/proactive investigations has been the subject of discussion at the annual Conference of International Investigators.[150] The Conference acknowledged that agencies should put more emphasis on conducting proactive investigations as a preventive measure. Many at the Conference shared the opinion that improved information flow, identifying and monitoring allegation patterns, red flags, and actors in particular sectors, regions or countries needed to be essential parts of the proactive investigation process.[151]

283. However, a number of interviewees for the present report indicated that proactive investigation were not viewed as a core mandate of the oversight office function and, as such, these services were not properly equipped for such anti-fraud work, which would require specific expertise and training and additional resources.

284. It should be noted that the increased use in recent years of ERP systems and other computerized administration and management systems and databases, including sound investigation case management systems, provides more suitable grounds for conducting proactive and preventive fraud investigations, as they can provide the information, data-mining and analytical results required for such investigations.

285. **The importance of full implementation of the recommendations made in the previous JIU reports to strengthen preventive/proactive investigations is hereby reiterated. The experiences and progress made by some organizations in this area and good practices outside the United Nations system (such as at the African Development Bank, the European Investment Bank and the World Bank) should be drawn upon.**

D. Investigation case management system

286. In most organizations with a substantive investigative workload, a case management system is paramount in the effective planning and administering of ongoing cases but also for the analysis of information and data collected through previous investigations. The system would usually include information on all allegations and investigations conducted in the organization and their outcome, irrespective of whether or not those investigations were done by the investigation office or another unit in the organization, and would provide data from the receipt of

[149] JIU/REP/2011/7, para. 9; JIU/REP/2000/9, paras. 71-75.
[150] At the 2014 and 2015 conferences.
[151] JIU/REP/2011/7, para. 9.

the allegation to the end of the investigation process. It also would support follow-up on the investigation report, including, disciplinary measures, sanctions and referrals of cases to national law enforcement authorities for criminal and civil procedures and asset recovery.

287. A number of investigation offices reviewed have an automated case management system in place, some of which are more advanced than others (see chap. VIII above); however, this is not always the case with other units who may be conducting investigations, such as discipline units, human resources and legal offices. Although fraud information may be available in different offices within the organization, it is not accessible in a user-friendly and consolidated manner and most often requires manual consolidation and retrieval.

288. This incomplete picture of organization-wide information on fraud allegations, ongoing and completed investigations and follow-up, does not allow for documenting the different allegations and cases and "connecting the dots". This impedes informed decision-making, proper follow-up on investigation cases, facilitation of feedback loops, and lessons learned.

289. The investigation division of OIOS of the United Nations Secretariat has taken action to improve its case management system by introducing a new automated system (GoCase, see box 6 below) as of September 2015. It is expected that the system will allow better collection, documentation and analysis of investigation-related data. It will allow for advanced research and facilitate intake process, as well as follow-up on investigation reports. It should be noted, however, that while the OIOS GoCase system has the technical capacity to function as a central intake system, there is currently no scope for the system to operate in this manner.[152]

Box 6: Investigation case management software: the example of GoCase

The GoCase software has been developed by UNODC as an investigation case management tool for use by Member States' law enforcement, investigative, intelligence and prosecution agencies. The functionality of GoCase to receive, input, store, validate, collate, analyse, retrieve and manage the information systematically is one of its biggest advantages. Such a software suite can have a significant impact on the outcome of an investigation and strengthen the documentation of cases with regard to the subsequent presentation at administrative tribunals. This is especially so in complex fraud cases, which can be very resource demanding.

290. **United Nations system organizations should consider the implementation of an investigation case management system, based on the volume, frequency and/or complexity of cases. The system should support a centralized intake mechanism, and the processing/management of information received from decentralized investigations and other units that may be conducting preliminary assessments. The system should be used as a central depository for capturing information and data for all allegations and investigations related fraud (and other misconduct), as well as their outcome and follow-up actions taken.**

[152] A/70/284, para. 64.

X. DISCIPLINARY MEASURES AND SANCTIONS (PILLAR 7)

291. Comprehensive disciplinary measures and sanction mechanisms to address substantiated fraud cases serve to decide on a punitive action for an individual's or third party's fraudulent behaviour and also serve as a deterrent to similar acts being committed in the future. Hence sanctions are an essential element for establishing a robust anti-fraud culture and commitment to combating fraud. Sanctions ensure, together with other anti-fraud measures, that the damage to the organization is kept to a minimum and risks for similar fraud schemes are mitigated.

A. Disciplinary process for staff members committing fraud

292. As part of their framework to detect and prevent fraud and corruption, most of the United Nations system organizations have policies and processes in place to determine the appropriate disciplinary measure that should be implemented in cases of proven fraud (and other misconduct) committed by staff members. The process is codified in staff rules and regulations complemented, in most cases, by additional guidelines.

293. The procedures applied by the different United Nations system organizations in enforcing disciplinary measures vary in some respects but they follow a similar general approach as outlined below.

294. An investigation report, on a staff member committing fraud, may be submitted to different offices or staff members, such as the legal office, human resources, senior management and in some cases the executive head. The report is reviewed and recommendations or decisions are made as to whether: (a) to initiate a disciplinary process; and, if so, (b) to impose disciplinary and other measures, based on the particular circumstances of the individual case. In some organizations, several offices at different levels are involved and may participate in the process through consultation, recommendations or decisions. Ultimately, the report together with the recommendation(s) is submitted to the organization's executive head or deputy head, senior manager or the respective person with delegated authority for follow-up action. Usually, the legal office and other offices, as appropriate, are closely consulted throughout the process.

295. Disciplinary measures are imposed once the investigation of facts surrounding the case is concluded and the staff member has been notified in writing of the measures and charges imposed against her or him. Procedurally, the staff member is informed of his or her right to respond to such allegations and may decide to seek assistance of counsel in his or her defence. Some United Nations system organizations have established committees or boards for providing advisory support to the executive head and the officials with delegated authority on matters regarding the appropriate disciplinary measures to be imposed. For example, UNESCO, IMO, and UNIDO have the Joint Disciplinary Committee, IAEA has the Joint Disciplinary Board, ILO the Committee on Accountability, and ITU the Joint Advisory Committee.

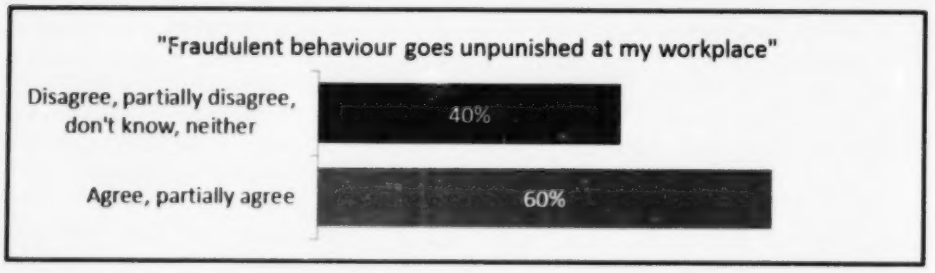
296. The staff member has the right of recourse against the disciplinary measure imposed, in accordance with the internal administration of justice process at the United Nations or ILO tribunals (the United Nations Dispute Tribunal, the United Nations Appeals Tribunal and the ILO Administrative Tribunal).

297. The review revealed that most organizations weigh the legal risks and related resource requirements in proportion to the gravity of the case when deciding if and what disciplinary measures to impose. Legal offices interviewed indicated they give careful consideration to any flaws or issues related to the conduct of the investigation, such as possible violations of due process and other procedural aspects and problems in gathering the required level of evidence and proof. Precedent is also considered to ensure consistency of the proposed penalty with similar previous cases.

298. As discussed above, the 2014 IAAC report[153] states that in some instances, cases were closed without the imposition of disciplinary action partly because it was believed that some of the cases would not hold in the face of the current justice system.

299. Cases closed without merited disciplinary action create an environment of impunity and send the wrong signal to the staff about the commitment of the organization to combat fraud. This situation was of great concern to many interviewees, including investigators, auditors, managers, human resources officers and ethics officer alike. It is also reflected in the JIU fraud survey where most than half of the respondents indicated they believe that fraudulent behaviour goes unpunished in their organization (see figure 9 below).

Figure 9: Fraudulent behaviour



Source: JIU fraud survey.

300. Of further concern was that, subsequent to the conclusion of an investigation, the imposition of a disciplinary action, if warranted, takes too long. As discussed below, these delays impede success of referrals and further the impunity of fraudsters.

[153] A/69/304.

B. Challenges of pursuing perpetrators

301. In most organizations interviewed, there were various incidents where the subject of allegation would resign and/or move to another organization prior to or during the investigation or disciplinary process. The Inspectors were informed that in most such cases disciplinary measures were not subsequently imposed against the individuals concerned, as the organization does not have the authority to enforce such measures on former staff members. In some organizations, a note may be placed in the personnel file of the former staff member indicating he/she was subject to an investigation or disciplinary process and that the case was not concluded.

302. Investigating units in a number of organizations reported that they have the discretion to continue investigations into possible misuses of human and financial resources, whether or not the subject is current or former personnel. However, once a staff member has resigned, he/she is no longer under the authority of the organization. As such, he/she could no longer be compelled to cooperate with an investigation that may be ongoing. Indeed, the United Nations Dispute Tribunal, in a ruling of 2010 on this issue, has held that an ex-staff member "cannot be compelled to be involved, let alone cooperate".[154] This could significantly impede the investigation, as it makes the collection and analysis of evidence much more difficult or even impossible. It was observed that other multinational entities have provisions in place ensuring former staff members' obligation to cooperate with the organizations in respect of investigations. Such provisions help to prevent staff members under investigation impeding the conduct of investigations by unilaterally disengaging from the organization.

303. **It is recommended that the executive heads of the United Nations system organizations instruct their respective legal offices to review the approach to cases where the subject of investigations resigns unilaterally, so as to ensure continuation of the investigations, as warranted, including the obligation of the subject to cooperate with the investigators, as well as recovery of damages, including from the staff members' pension, as appropriate** (the reader should also refer to paragraphs 306 to 327 below on referrals).

304. It was also disclosed during interviews that, owing to legal and confidentiality concerns, information on a staff member who is under investigation or has been disciplined, are not shared with other United Nations system organizations at the time of recruitment of this individual by another United Nations system organization. Some organizations are considering including questions in their job application forms requesting the applicant, in addition to the commonly used questions on previous criminal indictments, to provide information on possible investigation and disciplinary history with other employers along the lines "Have you been the subject of an investigation and/or disciplinary process of another employer, including by a United Nations system or international organization? If so,

[154] It was noted that, in most United Nations system organizations, if final entitlements are owing to a staff member, payment of such entitlements may be withheld to encourage the staff member to cooperate with the investigation. Depending on the amount of these entitlements, it may be the case; however, most of the persons interviewed in the context of this review did not see this provision as a strong tool to encourage cooperation, i.e. in major fraud cases where the amounts defrauded by far exceed the possible outstanding final entitlements.

please explain." The specific language is still under consideration in these organizations by legal and human resources offices.

305. **It is recommended that United Nations system organizations include in application forms specific questions on staff's previous involvement in fraudulent activities and the outcome of such activities and/or investigations. Any possible legal issues related to such action should be reviewed and cleared in advance by the legal office. Furthermore, the legal and human resources networks of HLCM should consult on a common approach and language to address this matter.**

Referral of cases to national judicial and enforcement authorities

306. In strengthening the disciplinary measures imposed by the United Nations system organizations, but also in view of the challenges in pursuing action against former staff members, referral of cases to national authorities, in particular for criminal and civil proceedings and/or for recovery of fraud losses, gain additional importance.

307. The United Nations cooperates with law enforcement and the judicial authorities of relevant Member States in accordance with its rights and obligations under the Convention on the Privileges and Immunities of the United Nations, adopted by the General Assembly on 13 February 1946, as well as other relevant international agreements and applicable legal principles.[155]

308. Section 21 of the Convention on the Privileges and Immunities of the United Nations ("the General Convention") stipulates that the United Nations should cooperate at all times with the appropriate authorities of Members to facilitate the proper administration of justice, secure the observance of regulations and prevent the occurrence of any abuse in connection with the privileges, immunities and facilities mentioned in article V of the General Convention. Moreover, in accordance with the Staff Regulations and Rules of the United Nations, officials and experts on mission, are required to comply with local laws and honour their private legal obligations.[156]

309. It is the policy of the United Nations that officials and experts on mission should be held accountable whenever they commit criminal acts, including fraud and corruption, not only because of the harm caused to the victims but also because they undermine the work and image of the United Nations. Consequently, where the United Nations, after proper internal investigation using its own investigative processes, establishes credible allegations that reveal that a crime may have been committed by United Nations officials or experts on mission, such allegations when proven credible are ordinarily brought to the attention of/referred to the Member State having jurisdiction over the alleged conduct. Given the legal issues involved in the referral to the relevant State, and the implication on the privileges and

[155] Report of the Secretary-General on Criminal accountability of United Nations officials and experts on mission (A/70/208), para. 33.

[156] Report of the Secretary-General on Information-sharing practices between the United Nations and national law enforcement authorities, as well as referrals of possible criminal cases related to United Nations staff, United Nations officials and experts on mission (A/63/331), paragraphs 2 and 3.

immunities of the United Nations, all such cases are reviewed by the OLA before a final determination is made on referring the case to authorities. OLA consults with the relevant programme managers, as appropriate, to determine the wider interests of the United Nations in pursuing a particular case.[157] OLA conducts referrals concerning all departments of the United Nations Secretariat, as well as all the funds and programmes of the United Nations.

310. When a decision is made to pursue a case, the United Nations refers credible allegations to law enforcement authorities by providing a written report on such allegations to the permanent mission of the Member State concerned for its appropriate action. In view of the inviolability of United Nations archives, set out in article II, section 4, of the General Convention, the United Nations provides the report on the allegations to the permanent mission on a voluntary basis, without prejudice to the privileges and immunities of the United Nations or its officials and experts on mission. In this way, the Secretary-General upholds the principle that such cooperation is not the result of, or subject to, any binding judicial process and that his decision on the nature and extent of the cooperation is a consequence of the determination of the Secretary-General that, in his sole opinion, the cooperation would not in any way prejudice the interests of the United Nations. Any follow-up requests for additional information or material and/or access to United Nations officials or experts on mission is generally made by the law enforcement authorities to the United Nations through the relevant permanent mission to the United Nations and are handled in accordance with the procedures outlined in a relevant report on the matter issued by the Secretary General (A/63/331).[158] It should be noted that once a case has been referred, it is up to the Member State authorities concerned to determine whether to pursue the matter, and whether the allegations, if proven, could constitute fraud under their laws.

311. If the law enforcement authorities of a Member State require formal testimony or wish to file criminal proceedings against a United Nations official or expert on mission in connection with a matter arising in the context of the official duties of that official or expert, a written request must be made to the Organization, generally through their permanent missions to the United Nations, for the waiver of immunities of the individual concerned. As provided in the United Nations Charter and section 20 of the General Convention "Privileges and immunities are granted to officials in the interests of the United Nations and not for the personal benefit of the individuals themselves. The Secretary-General shall have the right and the duty to waive the immunity of any official in any case where, in his opinion, the immunity would impede the course of justice and can be waived without prejudice to the interests of the United Nations."[159]

312. The specialized agencies follow similar procedures and practices. Depending on the particularities of the cases, agencies may decide to refer the cases to national authorities for further action and, exceptionally, consider waivers of immunity, if deemed appropriate.

[157] Ibid., see paragraphs 12 and 13.
[158] Ibid., see paragraph 14.
[159] Ibid, see paragraphs 19 to 25.

313. The United Nations General Assembly has established specific guidance on the matter of referrals for the Secretariat and its funds and programmes.[160] For example, resolution 70/114 requests, the Secretary-General "to bring credible allegations that reveal that a crime may have been committed by United Nations officials or experts on mission to the attention of the States against whose nationals such allegations are made and to request from those States updates ... on the status of their efforts to investigate and, as appropriate, prosecute crimes of a serious nature, as well as the types of appropriate assistance that States may wish to receive from the Secretariat for the purposes of such investigations and prosecutions."[161]

314. Further, in resolution 70/114, the General Assembly has expanded the Secretary-General's reporting obligations. In particular, paragraph 25 describes the information to be provided with respect to each case, as follows: "the United Nations entity involved, the year of referral, information about the type of crime and summary of allegations, status of investigations, prosecutorial and disciplinary actions taken, including with respect to individuals concerned who have left the duty mission or the service of the United Nations, any requests for waivers of immunity, as applicable, and information on jurisdictional, evidentiary or other obstacles to prosecution, while protecting the privacy of the victims as well as respecting the rights of those subject to the allegations".[162] The General Assembly requests that this information be provided for all referrals dating back to 1 July 2007, the year the Secretary-General began reporting on referrals.[163]

315. OLA informed the Inspectors that the United Nations will disclose to national authorities, on a case by case basis, documents and/or information regarding the cases, and immunity will be waived by the Secretary-General where immunity would impede the course of justice. Immunity can be waived without prejudice to the interests of the United Nations. Consequently, information obtained by the United Nations may be provided to the relevant authorities and documents may be shared, subject to consideration of privileges and immunities. Since the United Nations does not have any criminal or prosecutorial jurisdiction, the use of any information or documents provided, including their admissibility in any legal proceedings, is a matter for determination by the relevant judicial authorities to whom such information or documents have been provided.[164]

316. In resolution 62/63, as well as in subsequent resolutions on the criminal accountability of United Nations officials and experts on mission,[165] the General Assembly has consistently set the threshold for referral as "credible allegations" of criminal conduct.

317. In line with the threshold prescribed by the General Assembly, OLA commented for the present report that it does not require for allegations to be

[160] See i.e. General Assembly resolutions 62/63, 69/114 and 70/114.

[161] General Assembly resolution 70/114, op. 15.

[162] General Assembly resolution 70/114, op. 25.

[163] General Assembly resolution 70/114, op. 25; see also note by the United Nations Legal Counsel, as circulated to United Nations offices, funds and programmes on 1 February 2016; see most recent report prepared by the Secretary-General, Report of the Secretary-General on Criminal accountability of United Nations officials and experts on mission (A/70/208).

[164] See A/70/208, para. 33.

[165] See i.e. General Assembly resolutions 69/114 and 70/114.

proven and initiates referrals when the allegations are determined to be credible. Further, while investigative findings are necessary to determine the credibility of allegations, OLA commented that this does not necessitate the completion of an investigation into all aspects of the allegations. OLA notes, however, that the referral of credible allegations to national authorities requires the existence of evidence to substantiate the credibility of the allegations. Finally, OLA further indicated that referrals are not dependent on disciplinary processes and it is not the practice of the Secretariat and the separately administered funds and programmes to await the completion of disciplinary proceedings prior to effecting a referral.

318. However, as indicated in the 2014 IAAC report[166] and was confirmed by this review, in practice OLA makes referrals mostly on the basis of a substantiated allegation, which usually is expected to be based on a completed investigation. Considering that it may take up to 18 months to complete a complex investigation, OIOS strongly suggested that if, in "the course of its work, it determines that there is an allegation of serious criminal activity, it should be in a position to begin working with the national authorities immediately upon determining that the allegations were credible, without waiting for its investigation to be completed."[167] Even though this issue has been under consideration for several months by OIOS, OLA and other relevant offices, at the time of this review no decision had been made on the acceptance and implementation of the OIOS proposal.

319. Notwithstanding the above, most United Nations system legal offices interviewed on this matter were very direct in expressing reservations about the United Nations system's ability to effectively pursue cases with national authorities, citing the various risks posed by referrals, including legal and operational risks. The principle legal risk mentioned was the lifting of the United Nations immunities and privileges for pursuing and supporting civil and/or criminal proceedings before national courts and/or authorities, i.e. as it also concerns lifting the immunity of witnesses and related United Nations documents, and may expose the United Nations organizations to counterclaims.

320. For example, reference was made to a recent case by another multilateral institution (an MDB) involving a referral where a lower court ruled that the MDB concerned had, by virtue of the nature of its cooperation with national law enforcement authorities, including its participation in the investigations of such authorities, constructively waived its immunity from legal process. As explained, at the time of this writing, the case was before the supreme court of the country concerned. It was noted that, while proceedings in this case began in 2011, the merits of the underlying corruption allegations have not been adjudicated yet as of date, pending the resolution of the immunity issue.

321. It was further explained by a number of legal officers interviewed that referrals require legal expertise and advice that comes with costs to the organization. Referrals therefore also frequently looked at in the light of value for money and other practical, programmatic considerations, in addition to the legal issues.[168] It was also noted that referrals may not be appropriate in cases where there

[166] A/69/304, see paragraphs 52-54.

[167] A/69/304, paragraph 53.

[168] The United Nations Secretariat commented that this statement does not apply to them since referrals are made based on the guidance provided by the General Assembly resolutions.

are concerns as to the country in question not adhering to commonly accepted international human rights standards.

322. In view of these legal and procedural challenges and a concomitantly restrictive position taken by legal offices, referrals of cases throughout the United Nations system are very much an exception rather than the norm, reportedly even for cases that are well substantiated. Furthermore, as referrals are usually made after both the investigation and disciplinary process have been concluded, there is a long time lapse, sometimes several years, between the fraudulent or criminal conduct and the time action by a national authority could be initiated, which significantly lowers the success chances of adequately addressing and sanctioning the misconduct at national levels.[169]

323. Finally interviewees indicated that, once a referral is made, there is often no timely and/or adequate follow-up on the referrals by local authorities of Member States, or follow-up and tracking of the status of referrals by United Nations organizations. In this respect The General Assembly in resolution 70/114 states "Strongly urges States to take all appropriate measures to ensure that crimes by United Nations officials and experts on mission do not go unpunished and that the perpetrators of such crimes are brought to justice, without prejudice to the privileges and immunities of such persons and the United Nations under international law, and in accordance with international human rights standards, including due process."[170] It further "Encourages all States and the United Nations to cooperate with each other in the exchange of information and in facilitating the conduct of investigations and, as appropriate, the prosecution of United Nations officials and experts on mission who are alleged to have committed crimes of a serious nature, in accordance with their national law and applicable United Nations rules and regulations, fully respecting due process rights, as well as to consider strengthening the capacities of their national authorities to investigate and prosecute such crimes."[171]

Recovery of losses

324. As discussed above civil and criminal charges against the perpetrator and any recovery of asset and damages proceedings will only be possible (including in cases where arbitration is applied and arbitration decisions need to be enforced), by going through national authorities and courts, including for recovery of the staff member's pension. Reportedly, this makes recovery of assets, from losses and damages caused by the fraudulent act, extremely difficult. Interviewees explained this as the reason for the limited — and in most cases non-existent — recoveries of assets/damages in the United Nations system. In fact, a former staff member, despite proof by internal investigative processes that he/she has committed misconduct and/or fraud, would enjoy his/her pension in full (in addition to any fraudulent monetary gains), unless a final judgment by a national court is made in favour of the United Nations system organization. Such a favourable judgment would allow access, in some jurisdictions, to the pension of the staff member concerned for recovering fraud losses and

[169] This issue had been also highlighted by as the IAAC in relation to the United Nations Secretariat (see A/69/304, paras. 52-54).
[170] General Assembly resolution 70/114, op. 6.
[171] General Assembly resolution 70/114, op. 8.

assets.[172] Such a judgment may also provide an opportunity and basis for initiating possible civil proceedings to recover losses and damages from other assets of the convicted individual in certain jurisdictions under certain circumstances. However, for obtaining a possible favourable judgment for the United Nations system, a referral needs to be made with all the challenges and issues outlined above.

325. According to the information provided by OLA for the present report, the referrals for credible allegations of criminal conduct involving fraud amounted to a total of 61 cases from 2008 to 2014, with 24 referrals for the United Nations Secretariat and 37 for the fund and programmes. As explained by OLA, to the extend information is available there were two convictions during the same time period, though these convictions relate to fraud cases brought by Member States authorities without a prior referral by the United Nations. Available information on recovery of losses for the aforementioned time period relate only to fraud cases brought by Member States authorities without a prior referral by the United Nations; recovery amounted to US$ 932,165 in 2008, US$ 850,000 in 2009 and US$ 128,153 in 2012. The JIU was not able to obtain information on recovery of losses, if any, for the actual cases referred by OLA in the 2008 to 2014 timeframe. Also no information was provided on the number of actual convictions resulting from the referred cases.

326. It should also be noted that the BOA, in a recent report, highlighted that the majority of staff and external parties who committed fraud against the organizations were not typically pursued through the courts, and there was no clear policy on when such action should be contemplated, nor was there evidence that legal action was considered as a matter of course.[173] In a subsequent report, BOA assessed that the related recommendation[174] was not implemented and stated that "the Board has seen no evidence of the systematic legal pursuit of all proven cases of fraud".[175] BOA had also expressed concerns that "none of the losses to the value of US$9,354,949 stemming from fraud identified by the Internal Audit Division have been recovered to date, nor is legal action under way to pursue recovery of funds".[176] In response the Administration informed BOA that it had provided copies of the OIOS reports relating to the four cases in question to the Member States concerned. JIU was not in a position to obtain information on the current status of these cases.

---

[172] With respect to staff members convicted of crimes of which the United Nations was the victim, the Organization may seek, pursuant to article 45bis of the Regulations of the United Nations Joint Staff Pension Fund, a portion of a benefit payable to such person; recovery of assets from a staff member's pension from the Fund would be possible if the staff member expressed his or her formal consent to the recovery from the Fund.

[173] A/69/178, para. 69; A/69/5 (Vol. I), para. 150.

[174] "The Board recommends that the Administration develop a framework of actions and arrangements for the systematic legal pursuit of all proven cases of fraud", A/69/5 (Vol. I), para. 151.

[175] A/70/5 (Vol. I) and Corr.1, p. 69. It should be noted that the Administration has a different view in this regard stating, "the Administration notes that it already has a framework of actions and arrangements in place for the systematic pursuit of cases of fraud. Accordingly, the recommendation has already been implemented."

[176] Ibid., para. 125.

327. In the United Nations, in the context of disciplinary cases, recovery of financial losses to the organization from staff members is being effected under staff rule 10.1(b), which provides that, where conduct is determined by the Secretary-General to constitute misconduct and the organization has suffered a financial loss as a result of the staff member's actions, which are also determined to be wilful, reckless or grossly negligent, such staff member may be required to reimburse the organization for such loss in whole or in part. As explained for the present report, one of the proposed changes to the administrative instruction on investigation and disciplinary matters that is currently under revision by the Secretariat, is to elaborate on the procedures for calculation and recovery of losses to the organization resulting from established misconduct, pursuant to staff rule 10.1(b), so as to enhancing the legal framework to effect recovery. Similarly, UNIDO's Financial Rule 101.1.2 states: "Any staff member who contravenes the Financial Regulations or Rules or corresponding administrative instructions may be held personally accountable and financially liable for his or her action in accordance with Staff Rule 101.06".

328. For the reasons mentioned above, and in particular for promoting a strong message to potential fraudsters and instituting a robust anti-fraud culture, but also for sending a clear message of responsiveness to the public, the United Nations system needs to have effective mechanisms in place for following-up and sanctioning fraudulent staff members and third parties. This needs to include a clear protocol and procedures for referrals to national enforcement authorities and courts for criminal and civil proceedings, as well as for asset recovery, including the possibility of garnering the staff member's pension. The legal, reputational, financial, operational and political risks need to be weighted appropriately in this context guided by what is in the best interest of the United Nations system.

329. The implementation of the following recommendation is expected to enhance the effectiveness and efficiency of the organization's anti-fraud programme.

Recommendation 14

The executive heads of the United Nations system organizations, in consultation with the Office of Legal Affairs (OLA) of the United Nations, and their respective legal offices, should strengthen existing protocols and procedures for referrals of fraud cases (and other misconduct) to national enforcement authorities and courts for criminal and civil proceedings, as well as for asset recovery, and ensure that referrals are done in a timely and effective manner.

C. Vendor sanction regimes

330. Lack of vendor sanction policies and regimes leads to situations where the rules and processes for sanctions and corrective action are not clear and are confusing as to who decides, on what criteria and what due processes are to be followed. Imposing sanctions inconsistently and on an ad hoc basis poses legal risks and may invoke counterclaims by entities who believe that they have been unfairly blacklisted or otherwise sanctioned. A number of organizations such as UNDP,

UNOPS, UNFPA, UPU and FAO have vendor sanction regimes in place that apply to vendors, suppliers and commercial service providers contracted under procurement processes. Some of the vendor sanction regimes are based on the Model Policy Framework (MPF) of the CEB/HLCM.

331. The MPF provides a common basis for United Nations organizations to implement procedures for sanctioning suppliers who are involved in proscribed practices (corrupt, fraudulent, coercive, collusive and other unethical practices or obstruction). The objective of the MPF is to establish an ineligibility list that aggregates information disclosed by affected agencies, hosted by UNGM and accessible to designated staff of all participating organizations. The MPF was reviewed and agreed upon by the Legal Network of HLCM and endorsed by the Procurement Network in March 2011.

332. At the time of the review, several organizations, including UNHCR, WFP and UNRWA were in the process of revising and amending their vendor sanction policy, based on the MPF. WHO is considering adopting the MPF, but noted that the MPF-related establishment of a sanctions board and the corresponding procedures remain complex and challenging in nature. WHO, however, is fully engaged in cross-agency cooperation and sharing of vendor information (including with regard to actual or suspected fraud on the part of vendors), including as member of the Common Procurement Activities Group in Geneva and the HCLM Procurement Network. UNESCO follows the principles of United Nations harmonized vendor sanctioning; removal or suspension of vendors by UNESCO follows an internal review process, involving finance, legal and investigations units.

333. The MPF responds to the need for improved transparency, accountability and effectiveness in procurement. Since its approval by CEB, the number of organizations that have taken the necessary measures, including the establishment of vendor review committees to implement the provisions of the MPF, has continued to grow. Support among senior managers for harmonization of sanction regimes is quite strong according to the results of the JIU fraud survey, with 82 per cent in support (13 per cent neither agree nor disagree and 5 per cent partially disagree or disagree).

334. While it falls short of a full and automatic cross-debarment regime, which is a good practice among the MDBs, the MPF allows for a de facto cross-debarment that flags vendors for various types of sanctions (censure, ineligibility for registration, suspension etc.) with organizations retaining the right to opt-out.

335. In addition to harmonization efforts for punitive measures, the MPF also contains provisions for the rehabilitation of vendors. In fact, in the experience of UNDP,[177] one of the driving forces behind the MPF and an early adopter, the vast majority of cases are dealt with through administrative instead of legal processes, which is often more cost-efficient than lengthy legal procedures. It should be noted that, in contrast to the World Bank, the United Nations system, with a few exceptions such as UNOPS and UNDP, has opted not to publish its ineligibility list, reportedly at the suggestion of legal advisors.

[177] CEB, summary of conclusions of the seventeenth session of HLCM-PN, CEB/2015/HLCM_PN/17.

336. Staff interviewed for this report recognizes the MPF as a valuable framework to share information and a basis for common actions to sanction vendors. The Strategic Vendor Management Working Group of HLCM-PN, is currently establishing a workspace in UNGM where all participating organizations can share good practices and experiences, to be launched in 2016, in an effort to increase the number of United Nations organizations that adopt the MPF.

337. Another good practice identified is that of a vendor protest mechanisms, whereby competitors and vendors have the possibility to put in formal protests if they are of the view that the bidding process has not been conducted in accordance with the procurement policies. Protest mechanisms are particularly useful to uncover fraud, in cases of procurement vendor selection. Competitors are vigilant that due process is followed and can protest in cases of suspected collusion among certain vendors and/or vendors and procurement staff. Several United Nations organizations reviewed have such protest mechanisms in place. For example, UNFPA procurement has recently established a bid protest mechanism and the UNICEF Supply Division operates an ISO 9001-compliant quality management system, which manages receipt and follow-up to complaints. The United Nations Secretariat Procurement Division offers a mechanism via the Award Review Board for procurement challenges and complaints for unsuccessful bidders following the formal debrief of those that believe they have not been treated fairly.[178] FAO also maintains a vendor protest mechanism.

338. **It is recommended that the executive heads of United Nations system organizations, if they have not yet done so, adopt vendor sanction regimes based on the Model Policy Framework of the CEB/HLCM.**

D. Sanctioning of implementing partners

339. In most organizations reviewed, the legislative framework for the management of implementing partners does not provide for a specific formal sanction regime. However, the applicable guidance, agreements, memorandums of understanding and other instruments allow for certain anti-fraud activities and mitigating measures.[179] These include preventive measures, such as due diligence, requirements as to financial management, and payment in tranches based on receiving evidence and reports on the status of programme implementation. There are also audits, spot checks and other inspection and monitoring regimes that comprise oversight activities during programme implementation.

340. However, without detailed standardized provisions existing in sanctioning implementing partners, it is left up to the programme managers to decide on termination of engagements, stopping of payments or other punitive actions. The legal basis for such mitigating and "sanctioning" acts are in most cases in the contractual agreements with implementing partners, which may include the right of

[178] United Nations Secretariat, Procurement Division, www.un.org/Depts/ptd/complaints/complaints-guideline (accessed on 27 November 2015).

[179] At UNOPS, its definition of vendors is broader than the MPF and therefore includes implementing partners (see UNOPS organizational directive No. 41, para. 3.12).

the organization to stop funding for example when fraud is discovered, or to be reimbursed for damages to the organization.

341. FAO, UNHCR, UNFPA, UNIDO and WFP have provisions to that effect in their memorandums of understanding and agreements. However, while these provisions may have certain elements in place, such as termination and arbitration clauses, overall the framework for sanctioning implementing partners is fragmented and not robust. The criteria applied and the decision-making process, including whether decisions are taken by a panel or individual, and at what level, are not clear. There is also no formal framework for follow-up and enforcement of sanctions if imposed.

342. As the examples of the implementing partners fraud cases in Somalia show, despite the concluded and substantiated investigations by OIOS, and monetary losses of more than 9 million US$ to date no funds have been recovered. As indicated by the BOA in its latest report in respect to the aforementioned and related cases "Where fraud has been confirmed by the Investigations Division, the Administration has not yet activated the arbitration clauses within the project agreements to seek redress and restitution."[180] Occasionally, cases of referrals are more successful, such as a case originating from 2006 involving another organization, but also in this case, while the judgment of local courts was favourable to the organization, the funds have not yet been fully recovered.

343. In view of incomplete or lack of information on the matter of referrals and recovery of assets, concise data and evidence on the level of recovery of assets lost to fraud and the success ratio could not be collected and analysed for the present report. The questionnaire sent to all organizations had asked for information on recovered funds within the past five years. A review and analysis of the limited information provided, as well as that available in other oversight reports, i.e. of the internal and external auditors, indicates that the recoveries achieved are minimal if not nil.

344. Bearing in mind the significant funds transferred to implementing partners by some United Nations system organizations, as well as the high risk, including of fraud, of the implementation modality for implementing partners, the Inspectors wish to stress the importance of preventive anti-fraud measures, as outlined in above chapters on fraud control and detection. Also, organizations need to strengthen their reactive actions and sanction regime for implementing partners, for the similar reasons discussed above in relation to vendors and suppliers, for whom already a much more diligent and scrutinized process exists, including due process, competitive-bidding, involvement of committees and fraud prevention controls.

345. The sanction procedures for implementing partners should also apply to their subcontractors, as well as other partners who received funding from the United Nations system organizations, such as grantees. As discussed special focus on the particularities and sensitivities related to engaging and "sanctioning" government entities should be taken into account.

346. **It is recommended that the executive heads of United Nations system organizations, if they have not yet done so, update by the end of 2016 their**

[180] A/70/5 (Vol. I), para. 125.

implementing partner policies, procedures and related legal instruments to allow for sanctioning of implementing partners, including referrals of related fraud cases to national authorities and asset recovery.

E. Sharing information on sanctioning of third parties

347. The importance of sharing information among United Nations system organizations on third parties, vendors and suppliers and implementing partners, has been highlighted in previous JIU reports, and has been an issue of concern for oversight offices and donor Member States alike.

348. Regarding vendors and suppliers, good progress has been made on this front by many United Nations system organizations. For instance, within the Procurement Division of the United Nations Secretariat, sanctioned vendors are published on the Division's internal website accessible from within the United Nations system's network; sanctioned vendors are flagged in UNGM, which serves as the United Nations system's common vendor registration portal; a list of sanctioned vendors is sent to the Secretary of HLCM Procurement Network (HLCM-PN) and in turn shared with the HLCM-PN focal points of each United Nations organizations.

349. As discussed in chapter VII, section E, the main platform for sharing vendor related information is through the United Nations Global Market Place (UNGM).[181] Discussions are ongoing among United Nations system organizations, i.e. in the HLCM-PN to further developing UNGM to accommodate the registration and management of individual consultants. The UNGM membership was in general supportive of this initiative, especially in the light of the recent enhancement to the vendor eligibility filter that now checks against the consolidated lists of sanctioned vendors issued by the Security Council.[182]

350. Similar discussions have been initiated on expanding the UNGM to other partners, i.e. implementing partners. As noted at the twenty-eighth session of HLCM, the existing UNGM could be adjusted to track implementing partners in a similar way as it tracks suspect vendors, which could provide a platform for information-sharing. The Representatives of Internal Audit Services of the United Nations Organizations (UNRIAS) and the Representatives of the Investigation Services of the United Nations (UN-RIS) supported the HLCM plans for developing a common framework. They expressed willingness to continue to assist in the work as it moves forward. They supported the approach used by the UNGM on vendor eligibility and saw possibilities to apply it to implementing partners as well.

351. At the twenty-eighth session of HLCM the establishment of a task force was initiated, to include HLCM-PN and members of the former HACT advisory committee to: (a) develop a definition of use — when an NGO is considered a vendor, and when it should be considered as an implementing partner; (b) assess the feasibility of adapting UNGM as a platform to track fraud cases related to implementing partners; (c) explore alternative means of information sharing; (d) assess opportunities and limitations to expand areas currently covered by HACT assessments, and explore applicability of HACT risk management tools and

[181] See www.ungm.org; see also, on the status of UNGM, CEB/2015/HLCM_PN/17, para. 52.
[182] CEB/2015/HLCM_PN/17, para. 116.

instruments to vendors and implementing partners; (e) assess the value and feasibility of adapting procedures from the Vendor Eligibility Framework, as appropriate, for implementing partners; and (f) propose common approaches to mitigating risks.[183]

352. Interviewees have expressed different views on the functioning and performance of UNGM. Many noted that UNGM is working as expected, and it does allow for de facto cross-debarment, as information on sanctioned vendors is available. Some interviewees indicated that improvements were needed and the system could function as intended only insofar as that the data and information were being regularly updated by all United Nations organizations. This is an ongoing debate. In practice, organizations also review vendors against their own sanction list, which may be at times different, as different processes and criteria for sanctions exist among United Nations organizations. These are some of the challenges and show room for improvement of the system.

353. In addition to sharing information on sanctioned vendors through UNGM, a few organizations, such as UNDP and UNOPS, also provide information on sanctioned vendors on their websites, a practice also in place by the World Bank. Sanctioned vendors are published on the United Nations Secretariat Procurement Division's internal website accessible from within the United Nations system's network.

354. As outlined in a previous JIU report[184] and observed again during the conduct of this review, there is limited sharing of information on implementing partners at headquarters, regional and country levels. While some mechanisms and practices exist, i.e. exchanging implementing partner-related information at the operational management group/team of United Nations country team and under HACT, information-sharing is done ad hoc and often not in a systematic way. Additional mechanisms for sharing implementing partner-related information exist, however, under governance arrangements of pooled funds, and through the two Risk Management Units established for Somalia and Afghanistan.

355. The lack of proper information sharing on implementing partners, creates significant risks such as the possibility that a United Nations agency may engage an NGO that had been non-performing or involved in fraudulent acts in another agency. It may also allow for double-dipping of NGOs, not only in respect of funds received by different United Nations system organizations but also from other multilateral organizations such as the European Union, the MDBs and bilateral donors.

356. As the experience with the work of the Risk Management Unit[185] for Somalia shows, measures such as improved screening, due diligence, and sharing of

[183] CEB, conclusions of the twenty-eighth session of HLCM, CEB/2014/5.

[184] JIU/REP/2013/4.

[185] The Risk Management Unit (RMU) was established as part of the Resident Coordinator/Humanitarian Coordinator (RC/HC) office for Somalia to which it reports, and it provides operational advice on risk management issues to United Nations Country Team and RC/HC, and information on (implementing) partners engaged and contracted by the United Nations system organizations. To this end, the RMU has developed a database with contracts of 13 United Nations agencies (as of 2013) amounting to about US$ 419 million with about 1,200 IPs and partners. The database also allows checking any implementing partner against the United Nations Security Council sanctions lists and the World Bank vendor black-list.

implementing partner-related information, significantly help identify fraudulent and non-performing implementing partners and prevent the occurrence of similar fraud cases. As noted to the Inspectors, several ongoing and finalized fraud investigations of implementing partners in Somalia have been initiated based on information provided by the Unit, and as a result of the improved information sharing among United Nations system organizations in this context, including some of the cases mentioned above in paragraph 180.

357. In recent years, BOA and JIU have repeatedly highlighted the lack of coordination among United Nations system organizations operating in the same regions and using the same third parties. These organizations lack a formal mechanism to share information on partner performance.[186]

358. In response to these concerns, the Executive Committee of UNDG and CEB/HLCM had developed two task forces to consider the establishment of a formal requirement for sharing information on the performance of implementing partners.[187]

359. **It is recommended that the executive heads of United Nations system organizations, in their capacity as members of CEB, which oversees the development of UNGM, expedite their consideration of using UNGM as the platform for automated due diligence processes for implementing partners and consultants, as well as for comprehensive information-sharing on their performance among organizations.**

XI. PERFORMANCE REPORTING AND FEEDBACK (PILLAR 8)

A. Reporting on anti-fraud data and activities

Unreliable fraud reporting

360. Accurate data collection and reporting on fraud and fraud combating activities is an important part of controlling fraud against the United Nations system. The review revealed that fraud-related information and data contained in reports submitted to external auditors are often unreliable and confusing. For example, BOA in its concise summary for 2014 indicated that "the level of fraud and presumptive fraud reported by the operations of the United Nations as reported in volume I has also decreased, but many departments and offices failed to report the details of fraud cases identified in 2014. Consequently, the Board can provide no assurance that the amounts reported and disclosed by management in Volume I are complete or accurate."[188] A 2014 OIOS report[189] on fraud reporting in the United Nations Secretariat concluded in the same manner that information provide to external auditors may lack accuracy and thoroughness.

[186] A/70/322, para. 40; JIU/REP/2013/4, p. 43.

[187] A/70/322, para. 40; see also CEB/2014/5 (Conclusions of the Twenty-eighth Session of the High Level Committee on Management (HLCM)), paras 53-68.

[188] A/70/322, para. 44.

[189] OIOS, audit of the process of reporting cases of fraud or presumptive fraud in financial statements, report 2014/051.

361. Similarly, the number of fraud-related cases and data on fraud losses that were reported to the JIU by a number of organizations as part of this review were so different to the data that these organizations had officially submitted to external auditors that they were deemed unreliable for the purpose of analysis in the present report. For example, for the years 2012-2014, UNDP reported to the external auditors fraud-related losses that were markedly different than the amounts provided to the JIU. UNDP explained that it no longer reports the amount of loss sustained through procurement fraud, as it is in the process of developing a methodology that would allow a more accurate quantification of those losses. A task team has been created within UNDP to address this issue. It further explained that it did not report to the JIU the number of complaints that involved governmental and NGO implementing partners, as its case management system did not allow for the generation of those statistics at that time. The case management system is being updated to capture this type of information

362. The results of the JIU fraud survey across the United Nations system support the above observations. Forty-five per cent of survey respondents were not certain of their organization being forthcoming about fraud, particularly in releasing accurate statistics on substantiated cases, the type of fraud, disciplinary actions and other related data.

Lack of comprehensive management reporting on anti-fraud activities

363. In most organizations reviewed, reporting on anti-fraud related programmes and specifically on fraud risks and how they are being addressed are dispersed across various reports, such as the oversight annual report, the ethics office's report, the external auditor's report and financial statements of the organization and the head of organization's report on disciplinary measures. The plethora of reports originating from different offices makes it difficult for top management and governing bodies alike to obtain a clear picture of the extent to which the organization is exposed to fraud, the management of fraud risks and the level of fraud losses.

364. Furthermore, the review revealed a total lack of performance indicators in any of the current anti-fraud programmes in place throughout the United Nations system. Without a comprehensive understanding of the nature of fraud exposure, the adequacy of mitigation measures and applicable performance indicators, one cannot assess the effectiveness of anti-fraud activities or the efficient use of anti-fraud resources. As such, Member States may not be able to provide informed guidance and direction to the organizations on anti-fraud-related matters. This also does not allow for informed decision-making for setting acceptable risk appetite levels and agreeing on risk sharing modalities between the organizations and the Member States involved (see chap. V).

365. A comprehensive management report on the performance of anti-fraud activities consolidating the salient points of the various fraud-related reports and presented to the legislative and governing bodies by the organization's executive head, would provide for the required levels of accountability and transparency on fraud-related matters. Such a comprehensive fraud report needs to be taken into account systematically by the legislative/governing bodies in fulfilling their oversight responsibilities.

366. The implementation of the following recommendations is expected to enhance transparency and accountability as well as the effectiveness and efficiency of the organization's anti-fraud programme.

Recommendation 15

The executive heads of the United Nations system organizations should present to their legislative and governing bodies on an annual basis a consolidated and comprehensive management report on the performance of anti-fraud activities, based on key performance indicators. The report shall include, inter alia, the level of fraud exposure, status of compliance with anti-fraud policies, fraud statistics, sanctions imposed, fraud losses and recovery of assets, and lessons learned.

Recommendation 16

The legislative and governing bodies of the United Nations system organizations should: place on their respective agendas a permanent or standing item relating to fraud prevention, detection and response; review on an annual basis the consolidated and comprehensive management report presented by the executive head on anti-fraud policy and activities; and provide high-level guidance and oversight on fraud-related matters.

B. Lessons learned and feedback

367. In most United Nations system organizations, there is no systematic exercise of distilling and collecting lessons learned from fraud-related audit and investigations. While, in some cases, management letters are being prepared and sent to management with corrective actions as identified in audits and investigations, this, in practice, is not done in a structured and systematic manner, but rather ad hoc depending on the investigation teams in charge. What is lacking is the existence of a database, and ownership thereof, of what went wrong, the circumstances and the scheme of fraud, how it was discovered, the outcome, etc. There is also a lack of follow-up on the implementation of these recommendations and guidance, standard operating procedures, and a formal tracking of recommendations is absent.

368. Other multilateral organizations, such as the European Union and the World Bank, do share within their organizations the results of investigation and audit reports when they concern administrative and management issues, such as gaps in internal controls and areas for improvements, as part of the regular audit and/or investigation process and in line with specific guidelines to that effect. One example is the fraud-proofing exercise done by OLAF in consultation with other services (i.e. legal), where all existing and new European Union legislation, rules and regulations, or agreements and memorandums of understanding are periodically reviewed and updated, taking into consideration the relevant findings and recommendations of investigation reports, to continuously improve the legal instruments and close legal gaps. Another example is the casebook publication

issued by the World Bank, which describes the major and typical fraud cases and how they have been discovered and addressed, including lessons learned.

369. **There is need for United Nations system organizations to develop standard operating procedures that call for investigation and audit reports to be followed by systematic consideration of lessons learned regarding preventive and detective measures for improved anti-fraud activity. These lessons learned should be submitted for consideration to management.** A related recommendation in the JIU/REP/2000/9 report is hereby reiterated: Recommendation 5 "Executive heads should ensure that work programmes of units responsible for investigations include the development by management of preventive measures based on proactive investigations and lessons learned from completed investigations".

C. Audit and investigation functions interface

370. The review revealed that coordination and cooperation, including information-sharing, among the different oversight functions (audit, investigation, inspection and evaluation) needs to be further improved within the organization to effectively combat fraud. While most offices interviewed indicated that exchange of information is taking place, it is often done ad hoc and not in a consistent, timely and structured manner. The prevalent view is that auditors are neither mandated nor trained to do real forensic audits nor audit for fraud. Similarly, investigators usually dedicate little time or focus on controls and they are not trained in assessing the effectiveness of controls, in particular financial controls. Specific cases were mentioned where audit reports contained a number of obvious red flags, e.g. contract splitting, circumvention on controls and non-compliance with rules and procedures, that alone would warrant a fraud audit or investigation; but a systematic follow up was rarely done. Other examples provided were cases where auditors were not informed of ongoing investigations pertaining to a programme or country offices being audited.

371. It should be mentioned that a much closer interface between auditors and investigators was noticed in smaller internal oversight offices where it is not feasible to maintain separate internal audit and investigation units. The impediment of limited resources combined with the presence of dedicated multidisciplined professionals (auditors with investigation expertise and vice versa) under the leadership of experienced heads of office, have created the appropriate cross-feeding environment. Some interviewees, however, expressed a note of caution about auditors engaging extensively in fraud detection and/or becoming a part of an investigation team, as it is difficult to be seen as trusted staff when they return later to their purely internal audit role.

372. The need for improved coordination among the different oversight functions was also highlighted in a recent IAAC report that recommended that a review of the office of internal oversight of the United Nations Secretariat would, inter alia, "assess long-standing issues; opportunities to improve collaboration across the investigation, audit, and inspection and evaluation functions".[190]

[190] A/70/284, para. 65.

373. Clearly, effective collaboration and sharing of relevant information in a timely fashion among the different oversight functions is particularly important for successful anti-fraud work. It allows for synergies and complementarity among the diverse expertise and comparative advantages of the various oversight functions. The Inspectors wish to emphasize the importance of coordination in particular in the planning phase of both audits and investigations, where both functions will benefit from exchange of information. Where audits have identified red flags, consideration should be given systematically for a follow-up of these areas by the investigation function. Similarly, in certain cases, audit expertise should be available to the investigation team during the planning of or subsequent investigation of the cases. Furthermore, the investigation function should pay due attention to any weaknesses in anti-fraud systems and controls found during an investigation and, in coordination with the auditors, inform management to facilitate an appropriate follow up.

374. **It is recommended that the heads of oversight offices of United Nations system organizations enhance internal coordination and collaboration among the different oversight disciplines within their offices to strengthen anti-fraud activities and promote lessons learned. They should consider including a section on the status of such coordination in their existing report mechanisms to the legislative and governing bodies.**

D. Anti-fraud cooperation and coordination among entities

375. There is need to put in place mechanisms and procedures for enhancing cooperation and coordination among the United Nations system organizations to address fraud in a comprehensive manner and on a system-wide basis. As highlighted throughout the present report, areas for cooperation, coordination and collaboration include information-sharing on vendors and implementing partners, joint anti-fraud campaigns, sharing of training material, joint or parallel investigations, and harmonized sanctioning of staff and third parties. While there are commendable efforts underway in certain aspects of cooperation-as indicated in the report-, there is much room for improvement for anti-fraud work among organizations. Entities such as the United Nations Development Group (UNDG), the High-level Committee on Management (HLCM), the United Nations Representatives of Investigative Services (UN-RIS) and the Representatives of Internal Audit services (UNRIAS), should provide the fora for sharing experiences on fraud-related issues, and should dedicate appropriate time in their agendas for the serious discussion the subject of fraud deserves. Fraud is present throughout the United Nations system and combating fraud is an obligation not only of individual organizations but of the United Nations system as a whole.

ANNEXES I-IV

Annexes I-IV are published only on the JIU website (www.unjiu.org) together with the report

I. Compilation of fraud policies and other anti-fraud related policies
II. Definitions of fraud and presumptive fraud
III. Fraud risk assessments
IV. Survey Methodology

Attachment I

Fraud losses and numbers as reported in the financial statements to the organizations' external auditors from 2008 to 2014[191]

JIU Participating Organizations		2008-2009		2010-11		2012-13		2014	Subtotal/ Average for the years 2008-2014[192]
		2008	2009	2010	2011	2012	2013	2014	
United Nations Secretariat[193]	No. of fraud cases	21		9		18		5	53
	Value of cases	$730,049		$66,385		$11,876,000		$600,000	$13,272,434
	Overall expenditure	$9,280,000,000		$10,634,000,000		$10,631,000,000		$6,170,000,000	$36,725 millions
	Percentage	0.0079%		0.0006%		0.1117%		0.0097%	0.0325%
UNAIDS	No. of fraud cases	"no fraud cases"[194]		"no fraud cases"		"no fraud cases"	"no fraud cases"	"no fraud cases"	0
	Value of cases	0		0		0	0	0	0
	Overall expenditure	$524,100,000		$604,800,000		$575,100,000		$295,700,000	$1,999.7 millions
	Percentage	0%		0%		0%		0%	0%
UNCTAD	No. of fraud cases	no reference[195]	no reference	no reference	no reference	no reference	no reference	no reference	---
	Value of cases	no reference	no reference	no reference	no reference	no reference	no reference	no reference	---
	Overall expenditure	$37,000,000	$38,800,000	$39,200,000	$39,000,000	$36,000,000	$40,400,000	$38,800,000	$269.2 millions
	Percentage	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
ITC	No. of fraud cases	"no fraud cases"		"no fraud cases"		"no fraud cases"		"no fraud cases"	0
	Value of cases	0		0		0		0	0
	Overall expenditure	$129,453,000		$157,769,000,000		$155,580,000,000		$101,872,000,000	$415,350 millions
	Percentage	0%		0%		0%		0%	0%
UNDP	No. of fraud cases	29		16		27	38	27	137
	Value of cases	$3,260,000		$3,270,000		$5,900,000	$3,345,269	$3,350,000	$19,125,269
	Overall expenditure	$10,900,000,000		$11,430,000,000		$5,260,000,000	$5,240,000,000	$5,310,000,000	$38,140 millions
	Percentage	0.0299%		0.0286%		0.1122%	0.0638%	0.0631%	0.0595%
UNEP	No. of fraud cases	2		5		3		"no fraud cases"	10
	Value of cases	$933,393		$20,449		not provided		0	$953,842
	Overall expenditure	$682,700,000		$809,200,000		$751,400,000.00		$552,400,000	$2,795.7 millions
	Percentage	0.1367%		0.0025%		n/a		0%	0.0696%
UNFPA	No. of fraud cases	20		9		5	2	9	45
	Value of cases	$394,055		not provided[196]		not provided	$20,000	$20,000	$434,055
	Overall expenditure	$1,530,000,000		$1,650,000,000		$830,400,000	$913,300,000	$1,002,100,000	$5,925.8 millions
	Percentage	0.0258%		n/a		n/a	0.0022%	0.0020%	0.01%

[191] Source: as reported in the financial statements to the organizations' external auditors from 2008 to 2014.

[192] Based on the data provided for the years 2008 to 2014. The average percentage over the years 2008 to 2014 was calculated by dividing the sum of (bi)annual percentages for the years, where data was available, by the number of time periods where percentages were quantifiable. Whenever there were time periods for which fraud percentages were not determinable, "n/a" is stated, or added to the average percentage, respectively. Overall expenditure figures are rounded.

[193] Volume I of the BOA report for the United Nations Secretariat.

[194] "No fraud cases" indicates that the external audit report states that the number of fraud cases is zero.

[195] "No reference" indicates that the external audit report does not include a passage regarding fraud numbers/amounts.

[196] The external audit report provides some information on fraud or presumptive fraud (either the number of the amount of fraud). "Not provided" indicates that the fraud number, or amount, respectively, is not provided in the document.

JIU Participating Organizations		2008-2009		2010-11		2012-13		2014	Subtotal/ Average for the years 2008-2014[197]
		2008	2009	2010	2011	2012	2013	2014	
UN-Habitat	No. of fraud cases	2		1		1		1	5
	Value of cases	$66,211		$47,000		$243,233		"no financial loss"	$356,444
	Overall expenditure	$296,400,000		$426,900,000		$348,642,000		$208,032,000	$1,071.9 millions
	Percentage	0.0223%		0.0110%		0.0698%		0%	0.0258%
UNHCR	No. of fraud cases	6	4	2	19	2	16	6	55
	Value of cases	$94,800	$13,065	$35,000	$67,000	189,240-224,000	15,000-261,000	$124,000	$678,485
						$206,620[197]	$138,000		
	Overall expenditure	$1,602,200,000	$1,759,900,000	$1,878,200,000	$2,181,100,000	$2,357,700,000	$2,972,000,000	$3,355,000,000	$16,106 millions
	Percentage	0.0059%	0.0007%	0.0019%	0.0031%	0.0088%	0.0046%	0.0037%	0.0041%
UNICEF	No. of fraud cases	29		32		30	20	32	143
	Value of cases	$146,418		$5,520,000		$145,737	$193,803	$1,800,000	$7,805,958
	Overall expenditure	$6,320,000,000		$7,420,000,000		$3,620,000,000	$4,090,000,000	$4,560,000,000	$26,010 millions
	Percentage	0.0023%		0.0744%		0.0040%	0.0047%	0.0395%	0.025%
UNODC	No. of fraud cases	1		"no fraud cases"		6		1	8
	Value of cases	$14,309		0		$23,598		$18,115	$56,022
	Overall expenditure	$496,099,000		$450,146,000		$523,000,000		$325,400,000	$1,795 millions
	Percentage	0.0029%		0%		0.0045%		0.0056%	0.0032%
UNOPS	No. of fraud cases	6		9		16	9	6	46
	Value of cases	not provided		$229,220		not provided	$85,758	$206,972	$521,950
	Overall expenditure	$2,258,000,000		$2,467,000,000		$676,600,000	$703,700,000	$666,600,000	$6,771.9 millions
	Percentage	n/a		0.0093%		n/a	0.0122%	0.0310%	0.0175% / n/a
UNRWA	No. of fraud cases	16		22		26	20	25	109
	Value of cases	$13,540		$20,256		$33,079	$20,000	$123,004	$209,879
	Overall expenditure	$1,578,000,000		$1,921,000,000		$991,600,000	$1,118,460,000	$1,298,490,000	$6,907.5 millions
	Percentage	0.0009%		0.0011%		0.0033%	0.0018%	0.0095%	0.0033%
UN-Women	No. of fraud cases				"no fraud cases"	"no fraud cases"	4	"no fraud cases"	4
	Value of cases				0	0	$667,548	0	$667,548
	Overall expenditure				$198,300,000	$235,900,000	$264,100,000	$270,530,000	$968.8 millions
	Percentage				0%	0%	0.2528%	0%	0.0632%
WFP	No. of fraud cases	15	not provided	not provided	not provided	not provided	not provided	not provided	not provided
	Value of cases	$570,000	$1,349,724	$382,458	$38,951	$99,533	$444,349	$850,436	$3,735,451
	Overall expenditure	$3,725,000,000	$4,228,100,000	$4,237,700,000	$4,016,800,000	$4,395,700,000	$4,514,800,000	$5,214,600,000	$30,333 millions
	Percentage	0.0153%	0.0319%	0.0090%	0.0010%	0.0023%	0.0098%	0.0163%	0.0122%
FAO	No. of fraud cases	28		26		9		6	69
	Value of cases	$90,199		not provided		not provided		not provided	n/a
	Overall expenditure	$2,189,063,000		$2,736,561,000		$2,484,904,000		$553,770,000	$7,964 millions
	Percentage	0.0041%		n/a		n/a		n/a	0.0041% / n/a

[197] For calculation purposes, the medium of the fraud amount range has been taken.

JIU Participating Organizations		2008-2009		2010-11		2012-13		2014	Subtotal/ Average for the years 2008-2014[192]
		2008	2009	2010	2011	2012	2013	2014	
IAEA	No. of fraud cases	6	1	1	3	4	4	3	22
	Value of cases	not provided	not provided	not provided	not provided	not provided	not provided	not provided	not provided
	Overall expenditure	€ 367,832,409	€ 404,399,761	€ 445,084,145	€ 404,200,000	€ 446,200,000	€ 456,900,000	€ 476,000,000	€ 3,000 millions
	Percentage	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
ICAO	No. of fraud cases	no reference	no reference	no reference	no reference	no reference	no reference	no reference	no reference
	Value of cases	no reference	no reference	no reference	no reference	no reference	no reference	no reference	no reference
	Overall expenditure	CAD 244,200,000	CAD 254,341,000	CAD 235,089,000	CAD 217,963,000	CAD 218,956,000	CAD 246,921,000	CAD 258,413,000	CAD 1,421 mill
	Percentage	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
ILO	No. of fraud cases	no reference		"no fraud cases"	"no fraud cases"	"no fraud cases"	"no fraud cases"	no reference	0
	Value of cases	no reference		0	0	0	0	no reference	0
	Overall expenditure	$1,174,500,000		$670,600,000	$755,700,000	$689,000,000	$801,000,000	$772,000,000	$4,863 millions
	Percentage	n/a		0%	0%	0%	0%	n/a	0% / n/a
IMO	No. of fraud cases	no reference	no reference	no reference	"no fraud cases"	"no fraud cases"	"no fraud cases"	"no fraud cases"	0
	Value of cases	no reference	no reference	no reference	0	0	0	0	0
	Overall expenditure	£76,162,321		£43,977,726	£45,993,046	£49,525,282	£47,606,734	£45,012,703	$308 millions
	Percentage	n/a		n/a	0%	0%	0%	0%	0% / n/a
ITU	No. of fraud cases	"no fraud cases"		"no fraud cases"	"no fraud cases"	"no fraud cases"	"no fraud cases"	"no fraud cases"	0
	Value of cases	0		0	0	0	0	0	0
	Percentage	0%		0%	0%	0%	0%	0%	0%
UNESCO	No. of fraud cases	no reference		no reference	"no fraud cases"	no reference	no reference	no reference	no reference
	Value of cases	no reference		no reference	0	no reference	no reference	no reference	0 / no reference
	Percentage	n/a		n/a	0%	n/a	n/a	n/a	0 / n/a
UNIDO	No. of fraud cases	no reference		1	no reference	no reference	no reference	6	7
	Value of cases	no reference		€ 12,700	no reference	no reference	no reference	€ 6,423	€ 19,123
	Overall expenditure	€ 390,053,200		€ 171,398,200	€ 190,092,600	€ 237,769,700	€ 239,811,800	€ 190,831,000	€ 1,420 millions
	Percentage	n/a		0.0074%	n/a	n/a	n/a	0.0034%	0.0054% / n/a
UNWTO	No. of fraud cases	no reference	no reference	no reference	no reference	no reference	no reference	no reference	no reference
	Value of cases	no reference	no reference	no reference	no reference	no reference	no reference	no reference	no reference
	Percentage	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
UPU	No. of fraud cases	"no fraud cases"	"no fraud cases"	no reference	no reference	no reference	no reference	no reference	0 / no reference
	Value of cases	0	0	no reference	no reference	no reference	no reference	no reference	0 / no reference
	Percentage	0%	0%	n/a	n/a	n/a	n/a	n/a	0% / n/a
WHO	No. of fraud cases	4		3.00		2	"no fraud cases"	5	14
	Value of cases	$259,689		not provided		not provided	0	not provided	not provided
	Overall expenditure	$3,941,550,000		$4,593,000,000		$2,080,000,000	$2,252,000,000	$2,316,000,000	$15,183 millions
	Percentage	0.0066%		n/a		n/a	0%	n/a	0.0033% / n/a
WIPO	No. of fraud cases	no reference		no reference	no reference	21	19	3	43
	Value of cases	no reference		no reference	no reference	not provided	not provided	not provided	n/a
	Overall expenditure	CHF 582,800,000		CHF 308,400 000	CHF 325,400,000	CHF 321,500,000	CHF 336,500,000	CHF 333,200,000	CHF 2,209.8 mill
	Percentage	n/a		n/a	n/a	n/a	n/a	n/a	n/a

JIU Participating Organizations		2008-2009		2010-11		2012-13		2014	Subtotal/ Average for the years 2008-2014[192]
		2008	2009	2010	2011	2012	2013	2014	
WMO	No. of fraud cases	no reference	no reference	no reference	no reference	"no fraud cases"	"no fraud cases"	"no fraud cases"	0
	Value of cases	no reference	no reference	no reference	no reference	0	0	0	0
	Overall expenditure	CHF 85,000,000	CHF 91,800,000	CHF 90,200,000	CHF 91,500,000	CHF 84,500,000	CHF 76,300,000	CHF 96,900,000	CHF 616.2 mill
	Percentage	n/a	n/a	n/a	n/a	0%	0%	0%	0% / n/a

Attachment 2

Overview of actions to be taken by participating organizations on the recommendations of the Joint Inspection Unit JIU/REP/2016/4

		Intended impact	United Nations, its funds and programmes																Specialized agencies and IAEA											
			CEB	United Nations*	UNAIDS	UNCTAD	ITC	UNDP	UNEP	UNFPA	UN-Habitat	UNHCR	UNICEF	UNODC	UNOPS	UNRWA	UN-Women	WFP	FAO	IAEA	ICAO	ILO	IMO	ITU	UNESCO	UNIDO	UNWTO	UPU	WHO	WIPO	WMO
Report	For action		☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	For information		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Recommendation 1		a, d	E	E																										
Recommendation 2		a		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 3		a, e		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 4		f, h		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 5		e, f		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 6		e, f		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 7		a, e		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 8		e, a		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 9		f, h		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 10		f, h		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 11		f, h		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 12		f, h		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 13		f, h		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 14		f, h		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 15		a		E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Recommendation 16		a, i		L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L

Legend: **L:** Recommendation for decision by legislative organ **E:** Recommendation for action by executive head

■ : Recommendation does not require action by this organization

Intended impact: **a:** enhanced transparency and accountability **b:** dissemination of good/best practices **c:** enhanced coordination and cooperation **d:** strengthened coherence and harmonization **e:** enhanced control and compliance **f:** enhanced effectiveness **g:** significant financial savings **h:** enhanced efficiency **i:** other.

* Covers all entities listed in ST/SGB/2002/11 other than UNCTAD, UNODC, UNEP, UN-Habitat, UNHCR and UNRWA.